REGULATION (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 13 June 2024

laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Articles 16 and 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee ([1]),

Having regard to the opinion of the European Central Bank ([2]),

Having regard to the opinion of the Committee of the Regions ([3]),

Acting in accordance with the ordinary legislative procedure ([4]),

Whereas:

(1) The purpose of this Regulation is to improve the functioning of the internal market by laying down a uniform legal framework in particular for the development, the placing on the market, the putting into service and the use of artificial intelligence systems (AI systems) in the Union, in accordance with Union values, to promote the uptake of human centric and trustworthy artificial intelligence (AI) while ensuring a high level of protection of health, safety, fundamental rights as enshrined in the Charter of Fundamental Rights of the European Union (the 'Charter'), including democracy, the rule of law and environmental protection, to protect against the harmful effects of AI systems in the Union, and to support innovation. This Regulation ensures the free movement, cross-border, of AI-based goods and services, thus preventing Member States from imposing restrictions on the development, marketing and use of AI systems, unless explicitly authorised by this Regulation.

(2) This Regulation should be applied in accordance with the values of the Union enshrined as in the Charter, facilitating the protection of natural persons, undertakings, democracy, the rule of law and environmental protection, while boosting innovation and employment and making the Union a leader in the uptake of trustworthy AI.

(3) AI systems can be easily deployed in a large variety of sectors of the economy and many parts of society, including across borders, and can easily circulate throughout the Union. Certain Member States have already explored the adoption of national rules to ensure that AI is trustworthy and safe and is developed and used in accordance with fundamental rights obligations. Diverging national rules may lead to the fragmentation of the internal market and may decrease legal certainty for operators that develop, import or use AI systems. A consistent and high level of protection throughout the Union should therefore be ensured in order to achieve trustworthy AI, while divergences hampering the free circulation, innovation, deployment and the uptake of AI systems and related products and services within the internal market should be prevented by laying down uniform obligations for operators and

([1]) OJ C 517, 22.12.2021, p. 56.
([2]) OJ C 115, 11.3.2022, p. 5.
([3]) OJ C 97, 28.2.2022, p. 60.
([4]) Position of the European Parliament of 13 March 2024 (not yet published in the Official Journal) and decision of the Council of 21 May 2024.

欧洲议会和理事会条例(EU) 2024/1689

2024年6月13日

制定人工智能统一规则并修订条例(EC) No 300/2008、(EU) No 167/2013、(EU) No 168/2013、(EU) 2018/858、(EU) 2018/1139 和 (EU) 2019/2144 以及指令2014/90/EU、(EU) 2016/797和(EU) 2020/1828(人工智能法案)

(与欧洲经济区相关的文本)

欧洲议会和欧盟理事会，

考虑到《欧洲联盟运行条约》，特别是其第16条和第114条，

考虑到欧盟委员会提出的提案，

在将立法法案草案转交国家议会后，

考虑到欧洲经济和社会委员会的意见(1)，

考虑到欧洲中央银行的意见(2)，

考虑到区域委员会的意见(3)，

按照普通立法程序(4)行事，

鉴于：

(1) 本条例的目的是通过制定统一的法律

特别是为了在联盟内依照联盟价值观开发、投放市场、投入使用和使用人工智能系统(AI系统)的框架，以促进以人为本和可信人工智能(AI)的采用，同时确保对《欧洲联盟基本权利宪章》("宪章")所载健康、安全、基本权利(包括民主、法治和环境保护)的高水平保护，防范AI系统在联盟内的有害影响，并支持创新。本条例确保基于AI的商品和服务跨境自由流动，从而防止成员国对AI系统的开发、营销和使用施加限制，除非本条例明确授权。

(2) 本条例应依照《宪章》所载的联盟价值观予以适用，促进

对自然人、企业、民主、法治和环境保护的保护，同时促进创新和就业，使联盟成为可信人工智能应用的领导者。

(3) 人工智能系统可以轻松部署于经济的众多领域和社会的许多方面，包括

跨越国界，并且可以轻易在整个联盟内流通。某些成员国已经探索通过国家规则以确保人工智能可信和安全，并按照基本权利义务进行开发和使用。各国规则的分歧可能导致内部市场分裂，并可能降低开发、进口或使用人工智能系统的运营者的法律确定性。因此，应确保在整个联盟内实现一致和高水平的保护，以实现可信人工智能，同时应通过为运营者制定统一义务来防止阻碍人工智能系统及相关产品和服务在内部市场自由流通、创新、部署和采用的差异，并

(1) OJ C 517, 22.12.2021， 第56页。
(2) OJ C 115, 11.3.2022， 第5页。
(3) OJ C 97, 28.2.2022， 第60页。
(4) 欧洲议会2024年3月13日的立场(尚未在官方公报上公布)以及理事会2024年5月21日的决定。

本译本由机器翻译生成，供快速理解条文与内部培训使用；
涉及合规判断或法律适用时，请咨询专业顾问，并以官方英文文本为准。
翻译您自己的文件，请选择桐鸾译馆 · https://www.ivyivy.com.cn
扫码关注服务号

guaranteeing the uniform protection of overriding reasons of public interest and of rights of persons throughout the internal market on the basis of Article 114 of the Treaty on the Functioning of the European Union (TFEU). To the extent that this Regulation contains specific rules on the protection of individuals with regard to the processing of personal data concerning restrictions of the use of AI systems for remote biometric identification for the purpose of law enforcement, of the use of AI systems for risk assessments of natural persons for the purpose of law enforcement and of the use of AI systems of biometric categorisation for the purpose of law enforcement, it is appropriate to base this Regulation, in so far as those specific rules are concerned, on Article 16 TFEU. In light of those specific rules and the recourse to Article 16 TFEU, it is appropriate to consult the European Data Protection Board.

(4) AI is a fast evolving family of technologies that contributes to a wide array of economic, environmental and societal benefits across the entire spectrum of industries and social activities. By improving prediction, optimising operations and resource allocation, and personalising digital solutions available for individuals and organisations, the use of AI can provide key competitive advantages to undertakings and support socially and environmentally beneficial outcomes, for example in healthcare, agriculture, food safety, education and training, media, sports, culture, infrastructure management, energy, transport and logistics, public services, security, justice, resource and energy efficiency, environmental monitoring, the conservation and restoration of biodiversity and ecosystems and climate change mitigation and adaptation.

(5) At the same time, depending on the circumstances regarding its specific application, use, and level of technological development, AI may generate risks and cause harm to public interests and fundamental rights that are protected by Union law. Such harm might be material or immaterial, including physical, psychological, societal or economic harm.

(6) Given the major impact that AI can have on society and the need to build trust, it is vital for AI and its regulatory framework to be developed in accordance with Union values as enshrined in Article 2 of the Treaty on European Union (TEU), the fundamental rights and freedoms enshrined in the Treaties and, pursuant to Article 6 TEU, the Charter. As a prerequisite, AI should be a human-centric technology. It should serve as a tool for people, with the ultimate aim of increasing human well-being.

(7) In order to ensure a consistent and high level of protection of public interests as regards health, safety and fundamental rights, common rules for high-risk AI systems should be established. Those rules should be consistent with the Charter, non-discriminatory and in line with the Union's international trade commitments. They should also take into account the European Declaration on Digital Rights and Principles for the Digital Decade and the Ethics guidelines for trustworthy AI of the High-Level Expert Group on Artificial Intelligence (AI HLEG).

(8) A Union legal framework laying down harmonised rules on AI is therefore needed to foster the development, use and uptake of AI in the internal market that at the same time meets a high level of protection of public interests, such as health and safety and the protection of fundamental rights, including democracy, the rule of law and environmental protection as recognised and protected by Union law. To achieve that objective, rules regulating the placing on the market, the putting into service and the use of certain AI systems should be laid down, thus ensuring the smooth functioning of the internal market and allowing those systems to benefit from the principle of free movement of goods and services. Those rules should be clear and robust in protecting fundamental rights, supportive of new innovative solutions, enabling a European ecosystem of public and private actors creating AI systems in line with Union values and unlocking the potential of the digital transformation across all regions of the Union. By laying down those rules as well as measures in support of innovation with a particular focus on small and medium enterprises (SMEs), including startups, this Regulation supports the objective of promoting the European human-centric approach to AI and being a global leader in the development of secure, trustworthy and ethical AI as stated by the European Council ([5]), and it ensures the protection of ethical principles, as specifically requested by the European Parliament ([6]).

([5]) European Council, Special meeting of the European Council (1 and 2 October 2020) — Conclusions, EUCO 13/20, 2020, p. 6.
([6]) European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies, 2020/2012(INL).

在《欧洲联盟运行条约》(TFEU)第114条的基础上，保障整个内部市场对压倒性公共利益理由和个人权利的统一保护。在本条例包含关于在执法目的下限制使用AI系统进行远程生物特征识别、在执法目的下使用AI系统对自然人进行风险评估以及在执法目的下使用AI系统进行生物特征分类方面个人数据保护的具体规则的范围内，适宜就这些具体规则将本条例建立在TFEU第16条的基础上。鉴于这些具体规则和对TFEU第16条的援引，适宜咨询欧洲数据保护委员会。

(4) 人工智能是一个快速演进的技术家族，有助于广泛的经济、环境和社会惠及各行各业和社会活动。通过改进预测、优化运营和资源配置，以及为个人和组织提供个性化数字解决方案，AI的使用可为各类企业提供关键竞争优势，并支持对社会和环境有益的结果，例如在医疗保健、农业、食品安全、教育和培训、媒体、体育、文化、基础设施管理、能源、运输和物流、公共服务、安全、司法、资源和能源效率、环境监测、生物多样性和生态系统的保护与恢复以及气候变化减缓和适应等方面。

(5) 与此同时，根据其具体应用、使用和技术发展水平的相关情况，人工智能可能产生风险，并对受联盟法律保护的公共利益和基本权利造成损害。此类损害可能是物质性或非物质性的，包括身体、心理、社会或经济损害。

(6) 鉴于人工智能可能对社会产生的重大影响以及建立信任的需要，人工智能及其监管框架必须依照《欧洲联盟条约》(TEU)第2条所载的联盟价值观、《条约》所载的基本权利和自由以及根据TEU第6条制定的《宪章》来发展。作为前提条件，人工智能应当是以人为本的技术。它应当作为服务于人类的工具，最终目标是增进人类福祉。

(7) 为确保在健康、安全和基本权利方面对公共利益的一致和高水平保护，应建立高风险人工智能系统的共同规则。这些规则应与《宪章》一致、不歧视，并符合联盟的国际贸易承诺。它们还应考虑《数字十年数字权利和原则欧洲宣言》以及人工智能高级别专家组(AI HLEG)《可信AI伦理准则》。

(8) 因此，需要一个制定人工智能统一规则的欧盟法律框架，以促进人工智能在内部市场的发展、使用和采纳，同时满足对公共利益的高水平保护，例如健康与安全以及对基本权利的保护，包括欧盟法律所承认和保护的民主、法治和环境保护。为实现该目标，应制定规范某些人工智能系统投放市场、投入使用和使用的规则，从而确保内部市场的顺畅运行，并使这些系统受益于商品和服务自由流动原则。这些规则应在保护基本权利方面清晰且有力，支持新的创新解决方案，促成一个由公共和私营主体组成的欧洲生态系统，按照欧盟价值观创建人工智能系统，并释放欧盟所有地区数字化转型的潜力。通过制定这些规则以及支持创新的措施，特别关注中小企业(SME)，包括初创企业，本条例支持促进欧洲以人为本的人工智能方法以及在开发安全、可信和合乎道德的人工智能方面成为全球领导者的目标，正如欧洲理事会(5)所述，并确保对伦理原则的保护，正如欧洲议会(6)特别要求的那样。

(5) 欧洲理事会，欧洲理事会特别会议(2020年10月1日和2日)--结论，EUCO 13/20,2020，第6页。(6) 欧洲议会2020年10月20日关于向委员会提出的有关人工智能、机器人及相关技术伦理方面框架建议的决议，2020/2012(INL)。

(9) Harmonised rules applicable to the placing on the market, the putting into service and the use of high-risk AI systems should be laid down consistently with Regulation (EC) No 765/2008 of the European Parliament and of the Council ([7]), Decision No 768/2008/EC of the European Parliament and of the Council ([8]) and Regulation (EU) 2019/1020 of the European Parliament and of the Council ([9]) (New Legislative Framework). The harmonised rules laid down in this Regulation should apply across sectors and, in line with the New Legislative Framework, should be without prejudice to existing Union law, in particular on data protection, consumer protection, fundamental rights, employment, and protection of workers, and product safety, to which this Regulation is complementary. As a consequence, all rights and remedies provided for by such Union law to consumers, and other persons on whom AI systems may have a negative impact, including as regards the compensation of possible damages pursuant to Council Directive 85/374/EEC ([10]) remain unaffected and fully applicable. Furthermore, in the context of employment and protection of workers, this Regulation should therefore not affect Union law on social policy and national labour law, in compliance with Union law, concerning employment and working conditions, including health and safety at work and the relationship between employers and workers. This Regulation should also not affect the exercise of fundamental rights as recognised in the Member States and at Union level, including the right or freedom to strike or to take other action covered by the specific industrial relations systems in Member States as well as the right to negotiate, to conclude and enforce collective agreements or to take collective action in accordance with national law. This Regulation should not affect the provisions aiming to improve working conditions in platform work laid down in a Directive of the European Parliament and of the Council on improving working conditions in platform work. Moreover, this Regulation aims to strengthen the effectiveness of such existing rights and remedies by establishing specific requirements and obligations, including in respect of the transparency, technical documentation and record-keeping of AI systems. Furthermore, the obligations placed on various operators involved in the AI value chain under this Regulation should apply without prejudice to national law, in compliance with Union law, having the effect of limiting the use of certain AI systems where such law falls outside the scope of this Regulation or pursues legitimate public interest objectives other than those pursued by this Regulation. For example, national labour law and law on the protection of minors, namely persons below the age of 18, taking into account the UNCRC General Comment No 25 (2021) on children's rights in relation to the digital environment, insofar as they are not specific to AI systems and pursue other legitimate public interest objectives, should not be affected by this Regulation.

(10) The fundamental right to the protection of personal data is safeguarded in particular by Regulations (EU) 2016/679 ([11]) and (EU) 2018/1725 ([12]) of the European Parliament and of the Council and Directive (EU) 2016/680 of the European Parliament and of the Council ([13]). Directive 2002/58/EC of the European Parliament and of the Council ([14]) additionally protects private life and the confidentiality of communications, including by way of providing conditions for any storing of personal and non-personal data in, and access from, terminal equipment. Those Union legal acts provide the basis for sustainable and responsible data processing, including where data sets include a mix of personal and non-personal data. This Regulation does not seek to affect the application of existing Union law governing the processing of personal data, including the tasks and powers of the independent supervisory authorities competent to monitor compliance with those instruments. It also does not affect the obligations of providers and deployers of AI systems in their role as data controllers or processors stemming from Union or national law on the protection of personal data in so far as the design, the development or the use of AI systems involves the processing of personal data. It is also appropriate to clarify that data subjects continue to enjoy all the

([7]) Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30).

([8]) Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC (OJ L 218, 13.8.2008, p. 82).

([9]) Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 (OJ L 169, 25.6.2019, p. 1).

([10]) Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (OJ L 210, 7.8.1985, p. 29).

([11]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

([12]) Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

([13]) Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89).

([14]) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

(9) 适用于高风险人工智能系统投放市场、投入使用和使用的统一规则，应与欧洲议会和理事会第(EC) No 765/2008号条例(7)、欧洲议会和理事会第768/2008/EC号决定(8)以及欧洲议会和理事会第(EU) 2019/1020号条例(9)(新立法框架)一致地制定。本条例规定的统一规则应跨行业适用，并且按照新立法框架，不应影响现有欧盟法律，特别是关于数据保护、消费者保护、基本权利、就业和劳动者保护以及产品安全的法律，本条例是对其的补充。因此，此类欧盟法律为消费者以及可能受到人工智能系统负面影响的其他人员提供的所有权利和救济，包括依据理事会第85/374/EEC号指令(10)对可能损害的赔偿，均不受影响并完全适用。此外，在就业和劳动者保护的背景下，本条例因此不应影响符合欧盟法律的关于就业和工作条件的社会政策欧盟法律和国家劳动法，包括工作中的健康与安全以及雇主与劳动者之间的关系。本条例也不应影响成员国和欧盟层面承认的基本权利的行使，包括罢工权或自由，或采取成员国特定劳资关系制度所涵盖的其他行动的权利，以及按照国家法律谈判、缔结和执行集体协议或采取集体行动的权利。本条例不应影响欧洲议会和理事会关于改善平台工作工作条件的指令中规定的旨在改善平台工作工作条件的条款。此外，本条例旨在通过确立具体要求与义务，包括在人工智能系统的透明度、技术文档和记录保存方面，加强此类现有权利和救济的有效性。此外，本条例对人工智能价值链中各类运营者施加的义务，不应影响符合欧盟法律的国家法律，当此类法律超出本条例范围或追求本条例所追求目标之外的合法公共利益目标时，具有限制某些人工智能系统使用的效力。例如，国家劳动法和关于未成年人(即18岁以下人员)保护的法律，考虑到联合国儿童权利委员会关于数字环境中儿童权利的第25号一般性意见(2021)，只要其并非专门针对人工智能系统且追求其他合法公共利益目标，就不应受本条例影响。

(10) 保护个人数据的基本权利尤其受到以下条例的保障：(EU) 2016/679(11)和欧洲议会和理事会第(EU) 2018/1725号(12)以及欧洲议会和理事会第(EU) 2016/680号指令(13)。欧洲议会和理事会第2002/58/EC号指令(14)还保护私人生活和通信的保密性，包括通过为在终端设备中存储个人和非个人数据以及从终端设备访问此类数据提供条件。这些欧盟法律文件为可持续和负责任的数据处理提供了基础，包括在数据集包含个人和非个人数据混合的情况下。本条例不寻求影响管辖个人数据处理的现有欧盟法律的适用，包括负责监督对这些文书遵守情况的独立监管机构的任务和权力。在人工智能系统的设计、开发或使用涉及个人数据处理的情况下，本条例也不影响人工智能系统提供者和部署者作为数据控制者或处理者根据欧盟或国家个人数据保护法律承担的义务。还应澄清，数据主体继续享有此类欧盟法律赋予他们的所有

(7) 欧洲议会和理事会2008年7月9日关于制定认可要求并废止第339/93号条例(EEC)的第765/2008号条例(EC)(OJ L 218, 13.8.2008, p.30)。

(8) 欧洲议会和理事会2008年7月9日关于产品营销共同框架并废除理事会第93/465/EEC号决定的第768/2008/EC号决定(OJ L 218, 13.8.2008, p.82)。

(9) 欧洲议会和理事会2019年6月20日关于市场监督和产品合规并修订指令2004/42/EC及条例(EC) No 765/2008和(EU) No 305/2011的条例(EU) 2019/1020(OJ L 169, 25.6.2019， 第1页)。

(10) 理事会1985年7月25日关于协调成员国有关缺陷产品责任的法律、法规和行政规定的指令85/374/EEC(OJ L 210, 7.8.1985， 第29页)。

(11) 欧洲议会和理事会2016年4月27日关于在个人数据处理方面保护自然人以及此类数据自由流动并废止指令95/46/EC的条例(EU) 2016/679(通用数据保护条例)(OJ L 119, 4.5.2016， 第1页)。

(12) 欧洲议会和欧盟理事会2018年10月23日关于欧盟机构、机关、办事处和部门处理个人数据时保护自然人以及此类数据自由流动的第(EU) 2018/1725号条例，并废止第(EC) No 45/2001号条例和第1247/2002/EC号决定(OJ L 295, 21.11.2018, p.39)。

(13) 欧洲议会和理事会2016年4月27日关于主管当局为预防、调查、侦查或起诉刑事犯罪或执行刑事处罚目的处理个人数据方面保护自然人以及此类数据自由流动并废止理事会框架决定2008/977/JHA的指令(EU) 2016/680(OJ L 119, 4.5.2016， 第89页)。

(14) 欧洲议会和理事会2002年7月12日关于电子通信领域个人数据处理和隐私保护的指令2002/58/EC(隐私和电子通信指令)(OJ L 201, 31.7.2002， 第37页)。

rights and guarantees awarded to them by such Union law, including the rights related to solely automated individual decision-making, including profiling. Harmonised rules for the placing on the market, the putting into service and the use of AI systems established under this Regulation should facilitate the effective implementation and enable the exercise of the data subjects' rights and other remedies guaranteed under Union law on the protection of personal data and of other fundamental rights.

(11) This Regulation should be without prejudice to the provisions regarding the liability of providers of intermediary services as set out in Regulation (EU) 2022/2065 of the European Parliament and of the Council ([15]).

(12) The notion of 'AI system' in this Regulation should be clearly defined and should be closely aligned with the work of international organisations working on AI to ensure legal certainty, facilitate international convergence and wide acceptance, while providing the flexibility to accommodate the rapid technological developments in this field. Moreover, the definition should be based on key characteristics of AI systems that distinguish it from simpler traditional software systems or programming approaches and should not cover systems that are based on the rules defined solely by natural persons to automatically execute operations. A key characteristic of AI systems is their capability to infer. This capability to infer refers to the process of obtaining the outputs, such as predictions, content, recommendations, or decisions, which can influence physical and virtual environments, and to a capability of AI systems to derive models or algorithms, or both, from inputs or data. The techniques that enable inference while building an AI system include machine learning approaches that learn from data how to achieve certain objectives, and logic- and knowledge-based approaches that infer from encoded knowledge or symbolic representation of the task to be solved. The capacity of an AI system to infer transcends basic data processing by enabling learning, reasoning or modelling. The term 'machine-based' refers to the fact that AI systems run on machines. The reference to explicit or implicit objectives underscores that AI systems can operate according to explicit defined objectives or to implicit objectives. The objectives of the AI system may be different from the intended purpose of the AI system in a specific context. For the purposes of this Regulation, environments should be understood to be the contexts in which the AI systems operate, whereas outputs generated by the AI system reflect different functions performed by AI systems and include predictions, content, recommendations or decisions. AI systems are designed to operate with varying levels of autonomy, meaning that they have some degree of independence of actions from human involvement and of capabilities to operate without human intervention. The adaptiveness that an AI system could exhibit after deployment, refers to self-learning capabilities, allowing the system to change while in use. AI systems can be used on a stand-alone basis or as a component of a product, irrespective of whether the system is physically integrated into the product (embedded) or serves the functionality of the product without being integrated therein (non-embedded).

(13) The notion of 'deployer' referred to in this Regulation should be interpreted as any natural or legal person, including a public authority, agency or other body, using an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity. Depending on the type of AI system, the use of the system may affect persons other than the deployer.

(14) The notion of 'biometric data' used in this Regulation should be interpreted in light of the notion of biometric data as defined in Article 4, point (14) of Regulation (EU) 2016/679, Article 3, point (18) of Regulation (EU) 2018/1725 and Article 3, point (13) of Directive (EU) 2016/680. Biometric data can allow for the authentication, identification or categorisation of natural persons and for the recognition of emotions of natural persons.

(15) The notion of 'biometric identification' referred to in this Regulation should be defined as the automated recognition of physical, physiological and behavioural human features such as the face, eye movement, body shape, voice, prosody, gait, posture, heart rate, blood pressure, odour, keystrokes characteristics, for the purpose of establishing an individual's identity by comparing biometric data of that individual to stored biometric data of individuals in a reference database, irrespective of whether the individual has given its consent or not. This excludes AI systems intended to be used for biometric verification, which includes authentication, whose sole purpose is to confirm that a specific natural person is the person he or she claims to be and to confirm the identity of a natural person for the sole purpose of having access to a service, unlocking a device or having security access to premises.

([15]) Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (OJ L 277, 27.10.2022, p. 1).

权利和保障，包括与仅基于自动化的个人决策(包括画像)相关的权利。本条例确立的关于人工智能系统投放市场、投入使用和使用的统一规则，应促进有效实施，并使数据主体能够行使欧盟个人数据保护法律和其他基本权利所保障的权利及其他救济。

(11) 本条例不影响欧洲议会和理事会条例(EU) 2022/2065(15)所规定的关于中介服务提供者责任的条款。

(12) 本条例中"人工智能系统"的概念应当明确界定，并应与

致力于人工智能的国际组织，以确保法律确定性，促进国际趋同和广泛接受，同时提供灵活性以适应这一领域的快速技术发展。此外，定义应基于人工智能系统的关键特征，这些特征将其与较简单的传统软件系统或编程方法区分开来，并且不应涵盖仅基于由自然人定义的规则自动执行操作的系统。人工智能系统的一个关键特征是其推断能力。这种推断能力是指获得输出(例如预测、内容、建议或决策)的过程，这些输出可以影响物理和虚拟环境，也指人工智能系统从输入或数据中推导出模型或算法或两者兼有的能力。在构建人工智能系统时实现推断的技术包括从数据中学习如何实现特定目标的机器学习方法，以及从编码知识或待解决问题任务的符号表示中进行推断的逻辑和知识方法。人工智能系统的推断能力超越了基本数据处理，因为它能够实现学习、推理或建模。"基于机器"一词是指人工智能系统在机器上运行。对显式或隐式目标的提及强调了人工智能系统可以按照明确定义的目标或隐式目标运行。人工智能系统的目标可能不同于人工智能系统在特定情境中的预期目的。就本条例而言，环境应被理解为人工智能系统运行的语境，而人工智能系统生成的输出反映人工智能系统执行的不同功能，并包括预测、内容、建议或决策。人工智能系统被设计为以不同程度的自主性运行，这意味着它们在一定程度上独立于人类参与行动，并具有在无人工干预情况下运行的能力。人工智能系统在部署后可能表现出的适应性是指自学习能力，允许系统在使用过程中发生变化。人工智能系统可以独立使用，也可以作为产品的组件使用，无论该系统是物理集成到产品中(嵌入式)还是在不集成到产品中的情况下服务于产品的功能(非嵌入式)。

(13) 本条例中提及的"部署者"概念应解释为任何在其权限下使用人工智能系统的自然人或法人，包括

公共机构、机关或其他机构，但人工智能系统用于个人非职业活动的情形除外。根据人工智能系统的类型，系统的使用可能影响部署者以外的人员。

(14) 本条例中使用的"生物特征数据"概念应参照生物特征数据的概念来解释，

该概念界定于条例(EU) 2016/679第4条第(14)项、条例(EU) 2018/1725第3条第(18)项和指令(EU) 2016/680第3条第(13)项。生物特征数据可用于自然人的认证、识别或分类，以及自然人情绪的识别。

(15) 本条例中提及的"生物特征识别"概念应界定为自动化识别

基于人的身体、生理和行为特征，如面部、眼动、体型、声音、韵律、步态、姿态、心率、血压、气味、击键特征，通过将该个体的生物特征数据与参考数据库中个体的已存储生物特征数据进行比较，以确定个体身份，无论该个体是否已给予同意。这不包括旨在用于生物特征验证(包括身份认证)的人工智能系统，其唯一目的是确认某一特定自然人是否为其所声称的人，以及仅为访问服务、解锁设备或进入场所的安全访问之目的而确认自然人的身份。

(15) 欧洲议会和理事会2022年10月19日关于数字服务单一市场并修订指令2000/31/EC的条例(EU) 2022/2065(数字服务法案)(OJ L 277, 27.10.2022， 第1页)。

(16) The notion of 'biometric categorisation' referred to in this Regulation should be defined as assigning natural persons to specific categories on the basis of their biometric data. Such specific categories can relate to aspects such as sex, age, hair colour, eye colour, tattoos, behavioural or personality traits, language, religion, membership of a national minority, sexual or political orientation. This does not include biometric categorisation systems that are a purely ancillary feature intrinsically linked to another commercial service, meaning that the feature cannot, for objective technical reasons, be used without the principal service, and the integration of that feature or functionality is not a means to circumvent the applicability of the rules of this Regulation. For example, filters categorising facial or body features used on online marketplaces could constitute such an ancillary feature as they can be used only in relation to the principal service which consists in selling a product by allowing the consumer to preview the display of the product on him or herself and help the consumer to make a purchase decision. Filters used on online social network services which categorise facial or body features to allow users to add or modify pictures or videos could also be considered to be ancillary feature as such filter cannot be used without the principal service of the social network services consisting in the sharing of content online.

(17) The notion of 'remote biometric identification system' referred to in this Regulation should be defined functionally, as an AI system intended for the identification of natural persons without their active involvement, typically at a distance, through the comparison of a person's biometric data with the biometric data contained in a reference database, irrespectively of the particular technology, processes or types of biometric data used. Such remote biometric identification systems are typically used to perceive multiple persons or their behaviour simultaneously in order to facilitate significantly the identification of natural persons without their active involvement. This excludes AI systems intended to be used for biometric verification, which includes authentication, the sole purpose of which is to confirm that a specific natural person is the person he or she claims to be and to confirm the identity of a natural person for the sole purpose of having access to a service, unlocking a device or having security access to premises. That exclusion is justified by the fact that such systems are likely to have a minor impact on fundamental rights of natural persons compared to the remote biometric identification systems which may be used for the processing of the biometric data of a large number of persons without their active involvement. In the case of 'real-time' systems, the capturing of the biometric data, the comparison and the identification occur all instantaneously, near-instantaneously or in any event without a significant delay. In this regard, there should be no scope for circumventing the rules of this Regulation on the 'real-time' use of the AI systems concerned by providing for minor delays. 'Real-time' systems involve the use of 'live' or 'near-live' material, such as video footage, generated by a camera or other device with similar functionality. In the case of 'post' systems, in contrast, the biometric data has already been captured and the comparison and identification occur only after a significant delay. This involves material, such as pictures or video footage generated by closed circuit television cameras or private devices, which has been generated before the use of the system in respect of the natural persons concerned.

(18) The notion of 'emotion recognition system' referred to in this Regulation should be defined as an AI system for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data. The notion refers to emotions or intentions such as happiness, sadness, anger, surprise, disgust, embarrassment, excitement, shame, contempt, satisfaction and amusement. It does not include physical states, such as pain or fatigue, including, for example, systems used in detecting the state of fatigue of professional pilots or drivers for the purpose of preventing accidents. This does also not include the mere detection of readily apparent expressions, gestures or movements, unless they are used for identifying or inferring emotions. Those expressions can be basic facial expressions, such as a frown or a smile, or gestures such as the movement of hands, arms or head, or characteristics of a person's voice, such as a raised voice or whispering.

(19) For the purposes of this Regulation the notion of 'publicly accessible space' should be understood as referring to any physical space that is accessible to an undetermined number of natural persons, and irrespective of whether the space in question is privately or publicly owned, irrespective of the activity for which the space may be used, such as for commerce, for example, shops, restaurants, cafés; for services, for example, banks, professional activities, hospitality; for sport, for example, swimming pools, gyms, stadiums; for transport, for example, bus, metro and railway stations, airports, means of transport; for entertainment, for example, cinemas, theatres, museums, concert and conference halls; or for leisure or otherwise, for example, public roads and squares, parks, forests, playgrounds. A space should also be classified as being publicly accessible if, regardless of potential capacity or security restrictions, access is subject to certain predetermined conditions which can be fulfilled by an undetermined number of persons, such as the purchase of a ticket or title of transport, prior registration or having a certain age. In contrast, a space should not be considered to be publicly accessible if access is limited to specific and defined natural persons through either Union or national law directly related to public safety or security or through the clear manifestation

(16) 本条例所称"生物特征分类"的概念应定义为基于自然人的生物特征数据将其归入特定类别。此类特定类别可涉及性别、年龄、发色、眼睛颜色、纹身、行为或人格特征、语言、宗教、少数民族成员身份、性取向或政治取向等方面。这不包括纯粹作为另一商业服务固有附属功能且与该服务内在关联的生物特征分类系统，即该功能出于客观技术原因无法在脱离主服务的情况下使用，且该功能或特性的整合并非规避本条例规则适用性的手段。例如，在线市场上用于对面部或身体特征进行分类的滤镜可构成此类附属功能，因为它们只能在与主服务(即通过允许消费者预览产品在其本人身上的展示来销售产品并帮助消费者作出购买决定)相关的情况下使用。在线社交网络服务上用于对面部或身体特征进行分类以允许用户添加或修改图片或视频的滤镜也可被视为附属功能，因为此类滤镜无法脱离社交网络服务的主服务(即在线共享内容)而使用。

(17) 本 Regulation 中提及的"远程生物特征识别系统"概念应作功能性界定，

指旨在未经自然人主动参与的情况下识别自然人的AI系统，通常为远程方式，通过将某人的生物特征数据与参考数据库中包含的生物特征数据进行比较，无论所使用的特定技术、流程或生物特征数据类型如何。此类远程生物特征识别系统通常用于同时感知多个人或其行为，以便在未经自然人主动参与的情况下显著促进自然人的识别。这不包括旨在用于生物特征验证(包括身份认证)的人工智能系统，其唯一目的是确认某一特定自然人是否为其所声称的人，以及仅为访问服务、解锁设备或进入场所的安全访问之目的而确认自然人的身份。该排除的理由在于，与可用于在未经大量人员主动参与的情况下处理其生物特征数据的远程生物特征识别系统相比，此类系统对自然人基本权利的影响可能较小。对于"实时"系统，生物特征数据的采集、比较和识别均瞬时、近乎瞬时或在任何情况下无显著延迟地发生。在这方面，不应存在通过规定轻微延迟来规避本条例关于相关AI系统"实时"使用的规则的空间。"实时"系统涉及使用由摄像头或其他具有类似功能的设备生成的"实时"或"近实时"材料，如视频片段。相比之下，对于"事后"系统，生物特征数据已被采集，比较和识别仅在显著延迟之后发生。这涉及在系统对相关自然人使用之前已生成的材料，如闭路电视摄像头或私人设备生成的图片或视频片段。

(18) 本 Regulation 中提及的"情绪识别系统"概念应界定为一种人工智能系统，用于

基于自然人的生物特征数据识别或推断其情绪或意图的目的。该概念指幸福、悲伤、愤怒、惊讶、厌恶、尴尬、兴奋、羞耻、轻蔑、满足和愉悦等情绪或意图。它不包括身体状态，如疼痛或疲劳，例如包括用于检测职业飞行员或驾驶员疲劳状态以防止事故的系统。这也不包括仅检测明显可见的表情、手势或动作，除非它们被用于识别或推断情绪。这些表情可以是基本面部表情，如皱眉或微笑，或手势，如手、臂或头部的动作，或某人声音的特征，如提高的音量或低语。

(19) 就本 Regulation 而言，"可公开访问的空间"概念应理解为指任何

可供不确定数量的自然人进入的物理空间，无论该空间为私有还是公有，无论该空间可能用于何种活动，例如商业用途，如商店、餐厅、咖啡馆；服务用途，如银行、专业活动、酒店业；体育用途，如游泳池、健身房、体育场；交通用途，如公交、地铁和火车站、机场、交通工具；娱乐用途，如电影院、剧院、博物馆、音乐厅和会议厅；或休闲或其他用途，如公共道路和广场、公园、森林、游乐场。无论潜在容量或安保限制如何，如果进入须满足某些可由不确定数量的人满足的预定条件，如购买门票或车票、事先登记或达到一定年龄，则该空间也应被归类为可公开进入。相比之下，如果进入仅限于特定且确定的自然人，通过直接与公共安全或安保相关的欧盟或国家法律，或通过明确表明

of will by the person having the relevant authority over the space. The factual possibility of access alone, such as an unlocked door or an open gate in a fence, does not imply that the space is publicly accessible in the presence of indications or circumstances suggesting the contrary, such as. signs prohibiting or restricting access. Company and factory premises, as well as offices and workplaces that are intended to be accessed only by relevant employees and service providers, are spaces that are not publicly accessible. Publicly accessible spaces should not include prisons or border control. Some other spaces may comprise both publicly accessible and non-publicly accessible spaces, such as the hallway of a private residential building necessary to access a doctor's office or an airport. Online spaces are not covered, as they are not physical spaces. Whether a given space is accessible to the public should however be determined on a case-by-case basis, having regard to the specificities of the individual situation at hand.

(20) In order to obtain the greatest benefits from AI systems while protecting fundamental rights, health and safety and to enable democratic control, AI literacy should equip providers, deployers and affected persons with the necessary notions to make informed decisions regarding AI systems. Those notions may vary with regard to the relevant context and can include understanding the correct application of technical elements during the AI system's development phase, the measures to be applied during its use, the suitable ways in which to interpret the AI system's output, and, in the case of affected persons, the knowledge necessary to understand how decisions taken with the assistance of AI will have an impact on them. In the context of the application this Regulation, AI literacy should provide all relevant actors in the AI value chain with the insights required to ensure the appropriate compliance and its correct enforcement. Furthermore, the wide implementation of AI literacy measures and the introduction of appropriate follow-up actions could contribute to improving working conditions and ultimately sustain the consolidation, and innovation path of trustworthy AI in the Union. The European Artificial Intelligence Board (the 'Board') should support the Commission, to promote AI literacy tools, public awareness and understanding of the benefits, risks, safeguards, rights and obligations in relation to the use of AI systems. In cooperation with the relevant stakeholders, the Commission and the Member States should facilitate the drawing up of voluntary codes of conduct to advance AI literacy among persons dealing with the development, operation and use of AI.

(21) In order to ensure a level playing field and an effective protection of rights and freedoms of individuals across the Union, the rules established by this Regulation should apply to providers of AI systems in a non-discriminatory manner, irrespective of whether they are established within the Union or in a third country, and to deployers of AI systems established within the Union.

(22) In light of their digital nature, certain AI systems should fall within the scope of this Regulation even when they are not placed on the market, put into service, or used in the Union. This is the case, for example, where an operator established in the Union contracts certain services to an operator established in a third country in relation to an activity to be performed by an AI system that would qualify as high-risk. In those circumstances, the AI system used in a third country by the operator could process data lawfully collected in and transferred from the Union, and provide to the contracting operator in the Union the output of that AI system resulting from that processing, without that AI system being placed on the market, put into service or used in the Union. To prevent the circumvention of this Regulation and to ensure an effective protection of natural persons located in the Union, this Regulation should also apply to providers and deployers of AI systems that are established in a third country, to the extent the output produced by those systems is intended to be used in the Union. Nonetheless, to take into account existing arrangements and special needs for future cooperation with foreign partners with whom information and evidence is exchanged, this Regulation should not apply to public authorities of a third country and international organisations when acting in the framework of cooperation or international agreements concluded at Union or national level for law enforcement and judicial cooperation with the Union or the Member States, provided that the relevant third country or international organisation provides adequate safeguards with respect to the protection of fundamental rights and freedoms of individuals. Where relevant, this may cover activities of entities entrusted by the third countries to carry out specific tasks in support of such law enforcement and judicial cooperation. Such framework for cooperation or agreements have been established bilaterally between Member States and third countries or between the European Union, Europol and other Union agencies and third countries and international organisations. The authorities competent for supervision of the law enforcement and judicial authorities under this Regulation should assess whether those frameworks for cooperation or international agreements include adequate safeguards with respect to the protection of fundamental rights and freedoms of individuals. Recipient national

由对该空间拥有相关权限的人决定。仅仅存在事实上的进入可能性，例如门未上锁或围栏上的大门敞开，在存在相反迹象或情形(例如禁止或限制进入的标志)时，并不意味着该空间是公众可进入的。公司和企业场所，以及仅拟供相关员工和服务提供者进入的办公室和工作场所，属于非公众可进入的空间。公众可进入的空间不应包括监狱或边境管制。其他一些空间可能同时包含公众可进入和非公众可进入的空间，例如私人住宅楼中通往医生办公室或机场所必需的走廊。在线空间不属于涵盖范围，因为它们不是物理空间。然而，某一特定空间是否可供公众进入，应在个案基础上，结合手头具体情况的特点加以确定。

(20) 为了在保护基本权利、健康和安全的同时从人工智能系统中获得最大利益，并

为促进民主监督，人工智能素养应使提供者、部署者和受影响人员具备就人工智能系统作出知情决策的必要概念。这些概念可能因相关背景而异，可包括理解人工智能系统开发阶段技术要素的正确应用、使用期间应采取的措施、解释人工智能系统输出的适当方式，以及就受影响人员而言，理解借助人工智能作出的决策将如何对其产生影响所需的知识。在本条例适用的背景下，人工智能素养应为人工智能价值链中的所有相关行为者提供确保适当合规及其正确执行所需的洞见。此外，广泛实施人工智能素养措施并采取适当的后续行动，可有助于改善工作条件，并最终维持联盟可信人工智能的巩固与创新路径。欧洲人工智能委员会("委员会")应支持欧盟委员会推广人工智能素养工具、公众意识以及对使用人工智能系统的益处、风险、保障措施、权利和义务的理解。欧盟委员会和成员国应与相关利益相关者合作，推动制定自愿行为准则，以提升从事人工智能开发、运营和使用的人员的人工智能素养。

(21) 为确保公平竞争环境以及在整个 Union 内有效保护个人的权利和自由，本 Regulation 所确立的规则应以非歧视方式适用于人工智能系统的提供者，无论其设立于 Union 内还是第三国，并适用于设立于 Union 内的人工智能系统部署者。

(22) 鉴于其数字性质，某些人工智能系统应属于本 Regulation 的适用范围，即使它们

未在联盟投放市场、投入使用或使用。例如，设在联盟的运营者就某项将由符合高风险条件的人工智能系统执行的活动，向设在第三国的运营者外包某些服务，即属此种情形。在此情况下，该运营者在第三国使用的人工智能系统可处理在联盟合法收集并自联盟传输的数据，并向在联盟的订约运营者提供该人工智能系统由此处理产生的输出，而该人工智能系统并未在联盟投放市场、投入使用或使用。为防止规避本条例并确保对位于联盟的自然人的有效保护，本条例还应适用于设在第三国的人工智能系统提供者和部署者，前提是这些系统产生的输出拟在联盟使用。尽管如此，考虑到现有安排以及与交换信息和证据的外国伙伴未来合作的特殊需要，本条例不应适用于第三国公共当局和国际组织在联盟或国家层面为与联盟或成员国开展执法和司法合作而缔结的合作框架或国际协定范围内行事的情形，前提是相关第三国或国际组织在保护个人基本权利和自由方面提供充分保障。在相关情况下，这可涵盖第三国委托实体为支持此类执法和司法合作而执行特定任务的活动。此类合作框架或协定已在成员国与第三国之间，或欧洲联盟、Europol及其他联盟机构与第三国和国际组织之间双边建立。根据本条例负责监督执法和司法当局的主管机关应评估这些合作框架或国际协定是否在保护个人基本权利和自由方面包含充分保障。接收国

authorities and Union institutions, bodies, offices and agencies making use of such outputs in the Union remain accountable to ensure their use complies with Union law. When those international agreements are revised or new ones are concluded in the future, the contracting parties should make utmost efforts to align those agreements with the requirements of this Regulation.

(23) This Regulation should also apply to Union institutions, bodies, offices and agencies when acting as a provider or deployer of an AI system.

(24) If, and insofar as, AI systems are placed on the market, put into service, or used with or without modification of such systems for military, defence or national security purposes, those should be excluded from the scope of this Regulation regardless of which type of entity is carrying out those activities, such as whether it is a public or private entity. As regards military and defence purposes, such exclusion is justified both by Article 4(2) TEU and by the specificities of the Member States' and the common Union defence policy covered by Chapter 2 of Title V TEU that are subject to public international law, which is therefore the more appropriate legal framework for the regulation of AI systems in the context of the use of lethal force and other AI systems in the context of military and defence activities. As regards national security purposes, the exclusion is justified both by the fact that national security remains the sole responsibility of Member States in accordance with Article 4(2) TEU and by the specific nature and operational needs of national security activities and specific national rules applicable to those activities. Nonetheless, if an AI system developed, placed on the market, put into service or used for military, defence or national security purposes is used outside those temporarily or permanently for other purposes, for example, civilian or humanitarian purposes, law enforcement or public security purposes, such a system would fall within the scope of this Regulation. In that case, the entity using the AI system for other than military, defence or national security purposes should ensure the compliance of the AI system with this Regulation, unless the system is already compliant with this Regulation. AI systems placed on the market or put into service for an excluded purpose, namely military, defence or national security, and one or more non-excluded purposes, such as civilian purposes or law enforcement, fall within the scope of this Regulation and providers of those systems should ensure compliance with this Regulation. In those cases, the fact that an AI system may fall within the scope of this Regulation should not affect the possibility of entities carrying out national security, defence and military activities, regardless of the type of entity carrying out those activities, to use AI systems for national security, military and defence purposes, the use of which is excluded from the scope of this Regulation. An AI system placed on the market for civilian or law enforcement purposes which is used with or without modification for military, defence or national security purposes should not fall within the scope of this Regulation, regardless of the type of entity carrying out those activities.

(25) This Regulation should support innovation, should respect freedom of science, and should not undermine research and development activity. It is therefore necessary to exclude from its scope AI systems and models specifically developed and put into service for the sole purpose of scientific research and development. Moreover, it is necessary to ensure that this Regulation does not otherwise affect scientific research and development activity on AI systems or models prior to being placed on the market or put into service. As regards product-oriented research, testing and development activity regarding AI systems or models, the provisions of this Regulation should also not apply prior to those systems and models being put into service or placed on the market. That exclusion is without prejudice to the obligation to comply with this Regulation where an AI system falling into the scope of this Regulation is placed on the market or put into service as a result of such research and development activity and to the application of provisions on AI regulatory sandboxes and testing in real world conditions. Furthermore, without prejudice to the exclusion of AI systems specifically developed and put into service for the sole purpose of scientific research and development, any other AI system that may be used for the conduct of any research and development activity should remain subject to the provisions of this Regulation. In any event, any research and development activity should be carried out in accordance with recognised ethical and professional standards for scientific research and should be conducted in accordance with applicable Union law.

(26) In order to introduce a proportionate and effective set of binding rules for AI systems, a clearly defined risk-based approach should be followed. That approach should tailor the type and content of such rules to the intensity and scope of the risks that AI systems can generate. It is therefore necessary to prohibit certain unacceptable AI practices, to lay down requirements for high-risk AI systems and obligations for the relevant operators, and to lay down transparency obligations for certain AI systems.

在 Union 内使用此类输出的机关以及 Union 机构、机关、办事处和团体仍应承担责任，确保其使用符合 Union 法律。当这些国际协定在未来被修订或缔结新协定时，缔约方应尽最大努力使这些协定与本 Regulation 的要求保持一致。

(23) 本 Regulation 也应适用于作为提供者或AI系统的部署者。

(24) 如果且在一定程度上，人工智能系统在投放市场、投入使用或使用时，无论是否对此类用于军事、国防或国家安全目的的系统，无论开展这些活动的实体类型如何，例如是公共实体还是私人实体，均应被排除在本条例的适用范围之外。关于军事和国防目的，这种排除既由《欧洲联盟条约》第4(2)条证明合理，也由受国际公法约束的《欧洲联盟条约》第五编第二章所涵盖的成员国和联盟共同防务政策的特殊性证明合理，因此在涉及使用致命武力和其他军事和国防活动背景下的人工智能系统监管方面，国际公法是更合适的法律框架。关于国家安全目的，这种排除既由国家安全根据《欧洲联盟条约》第4(2)条仍属成员国专属责任这一事实证明合理，也由国家安全活动的特殊性质和运营需求以及适用于这些活动的特定国家规则证明合理。尽管如此，如果为军事、国防或国家安全目的开发、投放市场、投入使用或使用的人工智能系统在那些目的之外临时或永久用于其他目的，例如民用或人道主义目的、执法或公共安全目的，则该系统将属于本条例的适用范围。在这种情况下，将人工智能系统用于军事、国防或国家安全以外目的的实体应确保人工智能系统符合本条例，除非该系统已经符合本条例。为被排除的目的，即军事、国防或国家安全，以及一个或多个非排除目的，例如民用目的或执法，而投放市场或投入使用的人工智能系统属于本条例的适用范围，这些系统的提供者应确保符合本条例。在这些情况下，人工智能系统可能属于本条例适用范围这一事实不应影响开展国家安全、国防和军事活动的实体（无论开展这些活动的实体类型如何）为国家安全、军事和国防目的使用人工智能系统的可能性，这些使用被排除在本条例的适用范围之外。为民事或执法目的投放市场的人工智能系统，无论是否经过修改而用于军事、国防或国家安全目的，均不应属于本条例的适用范围，无论开展这些活动的实体类型如何。

(25) 本 Regulation 应支持创新，应尊重科学自由，且不应损害研究和开发活动。因此，有必要将仅为科学研究与开发这一唯一目的而专门开发并投入服务的人工智能系统和模型排除在其适用范围之外。此外，有必要确保本条例不以其他方式影响人工智能系统或模型在投放市场或投入服务之前的科学研究与开发活动。关于针对产品的人工智能系统或模型研究、测试和开发活动，本条例的规定也不应适用于这些系统和模型投入服务或投放市场之前。该排除不影响在因此类研究开发活动而使属于本条例适用范围的人工智能系统投放市场或投入服务时遵守本条例的义务，也不影响关于人工智能监管沙盒和在真实世界条件下测试的规定的适用。此外，在不影响将仅为科学研究与开发这一唯一目的而专门开发并投入服务的人工智能系统排除在外的情况下，任何其他可能用于开展任何研究开发活动的人工智能系统仍应受本条例规定约束。在任何情况下，任何研究开发活动均应按照公认的科学研究伦理和专业标准开展，并应依照适用的联盟法律进行。

(26) 为了对人工智能系统引入一套相称且有效的具有约束力的规则，应遵循明确界定的基于风险的方法。该方法应根据人工智能系统可能产生的风险的强度和范围，调整此类规则的类型和内容。因此，有必要禁止某些不可接受的人工智能实践，为高风险人工智能系统规定要求并为相关运营者规定义务，以及为某些人工智能系统规定透明度义务。

(27) While the risk-based approach is the basis for a proportionate and effective set of binding rules, it is important to recall the 2019 Ethics guidelines for trustworthy AI developed by the independent AI HLEG appointed by the Commission. In those guidelines, the AI HLEG developed seven non-binding ethical principles for AI which are intended to help ensure that AI is trustworthy and ethically sound. The seven principles include human agency and oversight; technical robustness and safety; privacy and data governance; transparency; diversity, non-discrimination and fairness; societal and environmental well-being and accountability. Without prejudice to the legally binding requirements of this Regulation and any other applicable Union law, those guidelines contribute to the design of coherent, trustworthy and human-centric AI, in line with the Charter and with the values on which the Union is founded. According to the guidelines of the AI HLEG, human agency and oversight means that AI systems are developed and used as a tool that serves people, respects human dignity and personal autonomy, and that is functioning in a way that can be appropriately controlled and overseen by humans. Technical robustness and safety means that AI systems are developed and used in a way that allows robustness in the case of problems and resilience against attempts to alter the use or performance of the AI system so as to allow unlawful use by third parties, and minimise unintended harm. Privacy and data governance means that AI systems are developed and used in accordance with privacy and data protection rules, while processing data that meets high standards in terms of quality and integrity. Transparency means that AI systems are developed and used in a way that allows appropriate traceability and explainability, while making humans aware that they communicate or interact with an AI system, as well as duly informing deployers of the capabilities and limitations of that AI system and affected persons about their rights. Diversity, non-discrimination and fairness means that AI systems are developed and used in a way that includes diverse actors and promotes equal access, gender equality and cultural diversity, while avoiding discriminatory impacts and unfair biases that are prohibited by Union or national law. Social and environmental well-being means that AI systems are developed and used in a sustainable and environmentally friendly manner as well as in a way to benefit all human beings, while monitoring and assessing the long-term impacts on the individual, society and democracy. The application of those principles should be translated, when possible, in the design and use of AI models. They should in any case serve as a basis for the drafting of codes of conduct under this Regulation. All stakeholders, including industry, academia, civil society and standardisation organisations, are encouraged to take into account, as appropriate, the ethical principles for the development of voluntary best practices and standards.

(28) Aside from the many beneficial uses of AI, it can also be misused and provide novel and powerful tools for manipulative, exploitative and social control practices. Such practices are particularly harmful and abusive and should be prohibited because they contradict Union values of respect for human dignity, freedom, equality, democracy and the rule of law and fundamental rights enshrined in the Charter, including the right to non-discrimination, to data protection and to privacy and the rights of the child.

(29) AI-enabled manipulative techniques can be used to persuade persons to engage in unwanted behaviours, or to deceive them by nudging them into decisions in a way that subverts and impairs their autonomy, decision-making and free choices. The placing on the market, the putting into service or the use of certain AI systems with the objective to or the effect of materially distorting human behaviour, whereby significant harms, in particular having sufficiently important adverse impacts on physical, psychological health or financial interests are likely to occur, are particularly dangerous and should therefore be prohibited. Such AI systems deploy subliminal components such as audio, image, video stimuli that persons cannot perceive, as those stimuli are beyond human perception, or other manipulative or deceptive techniques that subvert or impair person's autonomy, decision-making or free choice in ways that people are not consciously aware of those techniques or, where they are aware of them, can still be deceived or are not able to control or resist them. This could be facilitated, for example, by machine-brain interfaces or virtual reality as they allow for a higher degree of control of what stimuli are presented to persons, insofar as they may materially distort their behaviour in a significantly harmful manner. In addition, AI systems may also otherwise exploit the vulnerabilities of a person or a specific group of persons due to their age, disability within the meaning of Directive (EU) 2019/882 of the European Parliament and of the Council ([16]), or a specific social or economic situation that is likely to make those persons more vulnerable to exploitation such as persons living in extreme poverty, ethnic or religious minorities. Such AI systems can be placed on the market, put into service or used with the objective to or the effect of materially distorting the behaviour of a person and in a manner that causes or is reasonably likely to cause significant harm to that or another person or groups of persons, including harms that may be accumulated over time and should therefore be prohibited. It may not be possible to assume that there is an

([16]) Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services (OJ L 151, 7.6.2019, p. 70).

(27) 虽然基于风险的方法是一套相称且有效的具有约束力规则的基础，但必须回顾委员会任命的独立人工智能高级别专家组（AI HLEG）于2019年制定的可信人工智能伦理准则。在这些准则中，AI HLEG制定了七项不具约束力的人工智能伦理原则，旨在帮助确保人工智能可信且合乎伦理。这七项原则包括人的能动性和监督；技术稳健性和安全性；隐私和数据治理；透明度；多样性、非歧视和公平性；社会和环境福祉以及问责制。在不影响本条例和任何其他适用联盟法律具有法律约束力的要求的情况下，这些准则有助于设计连贯、可信和以人为本的人工智能，符合《宪章》和联盟赖以建立的价值观。根据AI HLEG的准则，人的能动性和监督意味着人工智能系统的开发和使用是作为服务于人的工具，尊重人的尊严和个人自主权，并以能够被人类适当控制和监督的方式运作。技术稳健性和安全性意味着人工智能系统的开发和使用方式允许在出现问题时保持稳健性，并抵御试图改变人工智能系统的使用或性能以允许第三方非法使用的行为，并最大限度地减少意外伤害。隐私和数据治理意味着人工智能系统的开发和使用符合隐私和数据保护规则，同时处理在质量和完整性方面达到高标准的数据。透明度意味着人工智能系统的开发和使用方式允许适当的可追溯性和可解释性，同时让人类意识到他们正在与人工智能系统通信或交互，并适当告知部署者该人工智能系统的能力和局限性以及受影响者的权利。多样性、非歧视和公平性意味着人工智能系统的开发和使用方式包括多元化的参与者并促进平等机会、性别平等和文化多样性，同时避免联盟或国家法律禁止的歧视性影响和不公平偏见。社会和环境福祉意味着人工智能系统以可持续和环境友好的方式开发和使用，并以造福全人类的方式开发和使用，同时监测和评估对个人、社会和民主的长期影响。这些原则的应用应尽可能体现在人工智能模型的设计和使用中。在任何情况下，它们都应作为根据本条例起草行为准则的基础。鼓励所有利益相关者，包括行业、学术界、民间社会和标准化组织，酌情考虑制定自愿最佳实践和标准的伦理原则。

(28) 除了人工智能的诸多有益用途外，它也可能被滥用，并为

操纵性、剥削性和社会控制性实践提供新颖而强大的工具。此类实践特别有害和具有滥用性，应予以禁止，因为它们违背了 Union 尊重人的尊严、自由、平等、民主和法治的价值观以及《宪章》所载的基本权利，包括不受歧视权、数据保护权、隐私权和儿童权利。

(29) 人工智能驱动的操纵技术可用于说服人们从事不想要的行为，或

通过以颠覆和损害其自主性、决策能力和自由选择的方式推动其作出决定来欺骗他们。将某些人工智能系统投放市场、投入使用或使用，其目的或效果是实质性扭曲人类行为，从而可能造成重大损害，特别是对身体健康、心理健康或经济利益产生足够严重的不利影响，此类人工智能系统尤其危险，因此应予以禁止。此类人工智能系统部署潜意识成分，如音频、图像、视频刺激，这些刺激是人们无法感知的，因为这些刺激超出人类感知范围，或其他操纵性或欺骗性技术，以人们无法有意识地察觉这些技术的方式颠覆或损害其自主性、决策能力或自由选择，或者即使人们察觉到了这些技术，仍然可能被欺骗或无法控制或抵抗它们。例如，机器-大脑接口或虚拟现实可以促进这一点，因为它们允许更高程度地控制向人们呈现的刺激，只要它们可能以显著有害的方式实质性扭曲其行为。此外，人工智能系统还可能以其他方式利用个人或特定群体因其年龄、欧洲议会和理事会指令(EU) 2019/882(16)含义内的残疾或特定社会或经济状况而产生的脆弱性，这些状况可能使这些人更容易被利用，例如生活在极端贫困中的人、族裔或宗教少数群体。此类人工智能系统可以被投放市场、投入使用或使用，其目的或效果是实质性扭曲个人行为，并以造成或合理可能造成对该人或另一人或群体重大损害的方式，包括可能随时间累积的损害，因此应予以禁止。可能无法假定存在

(16) 欧洲议会和理事会2019年4月17日关于产品和服务无障碍要求的指令(EU) 2019/882(OJ L 151, 7.6.2019, p.70)。

intention to distort behaviour where the distortion results from factors external to the AI system which are outside the control of the provider or the deployer, namely factors that may not be reasonably foreseeable and therefore not possible for the provider or the deployer of the AI system to mitigate. In any case, it is not necessary for the provider or the deployer to have the intention to cause significant harm, provided that such harm results from the manipulative or exploitative AI-enabled practices. The prohibitions for such AI practices are complementary to the provisions contained in Directive 2005/29/EC of the European Parliament and of the Council ([17]), in particular unfair commercial practices leading to economic or financial harms to consumers are prohibited under all circumstances, irrespective of whether they are put in place through AI systems or otherwise. The prohibitions of manipulative and exploitative practices in this Regulation should not affect lawful practices in the context of medical treatment such as psychological treatment of a mental disease or physical rehabilitation, when those practices are carried out in accordance with the applicable law and medical standards, for example explicit consent of the individuals or their legal representatives. In addition, common and legitimate commercial practices, for example in the field of advertising, that comply with the applicable law should not, in themselves, be regarded as constituting harmful manipulative AI-enabled practices.

(30) Biometric categorisation systems that are based on natural persons' biometric data, such as an individual person's face or fingerprint, to deduce or infer an individuals' political opinions, trade union membership, religious or philosophical beliefs, race, sex life or sexual orientation should be prohibited. That prohibition should not cover the lawful labelling, filtering or categorisation of biometric data sets acquired in line with Union or national law according to biometric data, such as the sorting of images according to hair colour or eye colour, which can for example be used in the area of law enforcement.

(31) AI systems providing social scoring of natural persons by public or private actors may lead to discriminatory outcomes and the exclusion of certain groups. They may violate the right to dignity and non-discrimination and the values of equality and justice. Such AI systems evaluate or classify natural persons or groups thereof on the basis of multiple data points related to their social behaviour in multiple contexts or known, inferred or predicted personal or personality characteristics over certain periods of time. The social score obtained from such AI systems may lead to the detrimental or unfavourable treatment of natural persons or whole groups thereof in social contexts, which are unrelated to the context in which the data was originally generated or collected or to a detrimental treatment that is disproportionate or unjustified to the gravity of their social behaviour. AI systems entailing such unacceptable scoring practices and leading to such detrimental or unfavourable outcomes should therefore be prohibited. That prohibition should not affect lawful evaluation practices of natural persons that are carried out for a specific purpose in accordance with Union and national law.

(32) The use of AI systems for 'real-time' remote biometric identification of natural persons in publicly accessible spaces for the purpose of law enforcement is particularly intrusive to the rights and freedoms of the concerned persons, to the extent that it may affect the private life of a large part of the population, evoke a feeling of constant surveillance and indirectly dissuade the exercise of the freedom of assembly and other fundamental rights. Technical inaccuracies of AI systems intended for the remote biometric identification of natural persons can lead to biased results and entail discriminatory effects. Such possible biased results and discriminatory effects are particularly relevant with regard to age, ethnicity, race, sex or disabilities. In addition, the immediacy of the impact and the limited opportunities for further checks or corrections in relation to the use of such systems operating in real-time carry heightened risks for the rights and freedoms of the persons concerned in the context of, or impacted by, law enforcement activities.

(33) The use of those systems for the purpose of law enforcement should therefore be prohibited, except in exhaustively listed and narrowly defined situations, where the use is strictly necessary to achieve a substantial public interest, the importance of which outweighs the risks. Those situations involve the search for certain victims of crime including missing persons; certain threats to the life or to the physical safety of natural persons or of a terrorist attack; and the localisation or identification of perpetrators or suspects of the criminal offences listed in an annex to this Regulation, where those criminal offences are punishable in the Member State concerned by a custodial sentence or a detention

([17]) Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') (OJ L 149, 11.6.2005, p. 22).

扭曲行为的意图，如果扭曲是由人工智能系统外部因素造成的，这些因素超出提供者或部署者的控制范围，即可能无法合理预见因此提供者或部署者无法缓解的因素。在任何情况下，提供者或部署者无需具有造成重大损害的意图，只要此类损害源于操纵性或利用性的人工智能赋能实践。对此类人工智能实践的禁止是对欧洲议会和理事会指令2005/29/EC(17)所含条款的补充，特别是导致消费者经济或财务损害的不公平商业行为在所有情况下均被禁止，无论它们是否通过人工智能系统或其他方式实施。本条例对操纵性和利用性实践的禁止不应影响医疗背景下的合法实践，如精神疾病的心理治疗或身体康复，当这些实践按照适用法律和医疗标准进行时，例如个人或其法定代表人的明确同意。此外，符合适用法律的常见和合法商业实践，例如在广告领域，本身不应被视为构成有害的操纵性人工智能赋能实践。

(30) 基于自然人生物特征数据的生物特征分类系统，例如个人的面部或指纹，以推断或推测个人的政治观点、工会成员身份、宗教或哲学信仰、种族、性生活或性取向，应予以禁止。该禁止不应涵盖依照联盟或国家法律获取的生物识别数据集根据生物识别数据进行的合法标记、过滤或分类，例如根据发色或眼睛颜色对图像进行分类，这例如可用于执法领域。

(31) 由公共或私人行为者提供对自然人进行社会评分的人工智能系统可能导致歧视性结果以及某些群体的排斥。它们可能侵犯尊严权和不歧视权以及平等和正义的价值观。此类人工智能系统基于与个人在多种情境下的社会行为相关的多个数据点，或在一定时期内已知、推断或预测的个人或人格特征，对自然人或其他群体进行评估或分类。从此类人工智能系统获得的社会评分可能导致自然人或其整个群体在社会情境中受到有害或不利待遇，这些情境与数据最初生成或收集的情境无关，或导致与其社会行为严重性不相称或不合理的有害待遇。因此，涉及此类不可接受评分实践并导致此类有害或不利结果的人工智能系统应予以禁止。该禁止不应影响依照联盟和国家法律为特定目的对自然人进行的合法评估实践。

(32) 在可公开访问的空间中使用人工智能系统对自然人进行"实时"远程生物特征识别出于执法目的，这种使用对相关人员的权利和自由具有特别的侵入性，因为它可能影响大部分人口的私生活，引发持续被监视的感觉，并间接阻止人们行使集会自由和其他基本权利。用于远程生物特征识别自然人的AI系统的技术不准确性可能导致有偏差的结果并产生歧视性影响。这种可能的有偏差结果和歧视性影响在年龄、族裔、种族、性别或残疾方面尤为相关。此外，在执法活动背景下或受执法活动影响时，此类实时运行系统的使用所带来的即时影响以及进一步检查或纠正机会有限，对相关人员的权利和自由构成更高风险。

(33) 因此，应禁止为执法目的使用这些系统，除非在穷尽列举的所列明且严格界定的情形，在这些情形中，使用对于实现重大公共利益严格必要，且该公共利益的重要性超过风险。这些情形涉及搜寻某些犯罪被害人，包括失踪人员；对自然人的生命或人身安全或恐怖袭击的某些威胁；以及定位或识别本条例附件所列刑事犯罪的实施者或嫌疑人，且这些刑事犯罪在相关成员国可处以最高至少四年的监禁或羁押

(17) 欧洲议会和理事会2005年5月11日关于内部市场中不公平企业对消费者商业行为的第2005/29/EC号指令，修订理事会第84/450/EEC号指令、欧洲议会和理事会第97/7/EC号、第98/27/EC号和第2002/65/EC号指令以及欧洲议会和理事会第(EC)第2006/2004号条例("不公平商业行为指令")(OJ L 149, 11.6.2005, p.22)。

order for a maximum period of at least four years and as they are defined in the law of that Member State. Such a threshold for the custodial sentence or detention order in accordance with national law contributes to ensuring that the offence should be serious enough to potentially justify the use of 'real-time' remote biometric identification systems. Moreover, the list of criminal offences provided in an annex to this Regulation is based on the 32 criminal offences listed in the Council Framework Decision 2002/584/JHA ([18]), taking into account that some of those offences are, in practice, likely to be more relevant than others, in that the recourse to 'real-time' remote biometric identification could, foreseeably, be necessary and proportionate to highly varying degrees for the practical pursuit of the localisation or identification of a perpetrator or suspect of the different criminal offences listed and having regard to the likely differences in the seriousness, probability and scale of the harm or possible negative consequences. An imminent threat to life or the physical safety of natural persons could also result from a serious disruption of critical infrastructure, as defined in Article 2, point (4) of Directive (EU) 2022/2557 of the European Parliament and of the Council ([19]), where the disruption or destruction of such critical infrastructure would result in an imminent threat to life or the physical safety of a person, including through serious harm to the provision of basic supplies to the population or to the exercise of the core function of the State. In addition, this Regulation should preserve the ability for law enforcement, border control, immigration or asylum authorities to carry out identity checks in the presence of the person concerned in accordance with the conditions set out in Union and national law for such checks. In particular, law enforcement, border control, immigration or asylum authorities should be able to use information systems, in accordance with Union or national law, to identify persons who, during an identity check, either refuse to be identified or are unable to state or prove their identity, without being required by this Regulation to obtain prior authorisation. This could be, for example, a person involved in a crime, being unwilling, or unable due to an accident or a medical condition, to disclose their identity to law enforcement authorities.

(34) In order to ensure that those systems are used in a responsible and proportionate manner, it is also important to establish that, in each of those exhaustively listed and narrowly defined situations, certain elements should be taken into account, in particular as regards the nature of the situation giving rise to the request and the consequences of the use for the rights and freedoms of all persons concerned and the safeguards and conditions provided for with the use. In addition, the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement should be deployed only to confirm the specifically targeted individual's identity and should be limited to what is strictly necessary concerning the period of time, as well as the geographic and personal scope, having regard in particular to the evidence or indications regarding the threats, the victims or perpetrator. The use of the real-time remote biometric identification system in publicly accessible spaces should be authorised only if the relevant law enforcement authority has completed a fundamental rights impact assessment and, unless provided otherwise in this Regulation, has registered the system in the database as set out in this Regulation. The reference database of persons should be appropriate for each use case in each of the situations mentioned above.

(35) Each use of a 'real-time' remote biometric identification system in publicly accessible spaces for the purpose of law enforcement should be subject to an express and specific authorisation by a judicial authority or by an independent administrative authority of a Member State whose decision is binding. Such authorisation should, in principle, be obtained prior to the use of the AI system with a view to identifying a person or persons. Exceptions to that rule should be allowed in duly justified situations on grounds of urgency, namely in situations where the need to use the systems concerned is such as to make it effectively and objectively impossible to obtain an authorisation before commencing the use of the AI system. In such situations of urgency, the use of the AI system should be restricted to the absolute minimum necessary and should be subject to appropriate safeguards and conditions, as determined in national law and specified in the context of each individual urgent use case by the law enforcement authority itself. In addition, the law enforcement authority should in such situations request such authorisation while providing the reasons for not having been able to request it earlier, without undue delay and at the latest within 24 hours. If such an authorisation is rejected, the use of real-time biometric identification systems linked to that authorisation should cease with immediate effect and all the data related to such use should be discarded and deleted. Such data includes

([18]) Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (OJ L 190, 18.7.2002, p. 1).

([19]) Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (OJ L 333, 27.12.2022, p. 164).

命令，且按该成员国法律界定。依照国家法律规定的此类监禁或羁押命令门槛有助于确保犯罪足够严重，从而可能为使用"实时"远程生物特征识别系统提供正当理由。此外，本条例附件提供的刑事犯罪清单基于理事会框架决定2002/584/JHA(18)所列的32项刑事犯罪，同时考虑到其中某些犯罪在实践中可能比其他犯罪更相关，因为对于实际追查定位或识别所列不同刑事犯罪的实施者或嫌疑人而言，诉诸"实时"远程生物特征识别在不同程度上可预见地可能是必要且相称的，并考虑到损害或可能负面后果在严重性、概率和规模上可能存在的差异。对自然人的生命或人身安全的紧迫威胁也可能源于欧洲议会和理事会指令(EU) 2022/2557(19)第2条第(4)点所定义的关键基础设施的严重中断，若此类关键基础设施的中断或毁坏会导致对个人生命或人身安全的紧迫威胁，包括通过对向民众提供基本供应或对国家核心职能的行使造成严重损害。此外，本条例应保留执法、边境管制、移民或庇护当局在相关人员在场时依照联盟和国家法律为此类检查规定的条件进行身份检查的能力。特别是，执法、边境管制、移民或庇护当局应能够依照联盟或国家法律使用信息系统，以识别在身份检查期间拒绝被识别或无法陈述或证明其身份的人员，而本条例不要求其获得事先授权。例如，这可能包括参与犯罪的人员因事故或医疗状况而不愿或无法向执法当局披露其身份。

(34) 为确保以负责任和相称的方式使用这些系统，同样重要的是

规定在每一个穷尽列举且严格界定的情形中，应考虑某些要素，特别是关于引发请求的情形性质、使用对所有相关人员权利和自由的后果以及使用所规定的保障措施和条件。此外，为执法目的在可公开访问的空间使用"实时"远程生物特征识别系统，应仅用于确认特定目标个人的身份，并应限于在时间期限以及地理和个人范围方面严格必要的限度内，尤其考虑到关于威胁、被害人或者实施者的证据或迹象。只有在相关执法当局已完成基本权利影响评估，且除本条例另有规定外，已按本条例规定将该系统登记在数据库中时，才应授权在可公开访问的空间使用实时远程生物特征识别系统。人员参考数据库应适合上述每一种情形中的每一使用案例。

(35) 每次为执法目的在可公开访问的空间中使用"实时"远程生物特征识别系统

执法应获得成员国司法当局或独立行政当局的明确且具体的授权，其决定具有约束力。此类授权原则上应在使用AI系统识别一人或多人之前获得。在出于紧急性的正当理由情形下，应允许对该规则有例外，即在使用有关系统的需要使得在开始使用AI系统之前获得授权实际上和客观上不可能的情形。在此类紧急情形中，AI系统的使用应限于绝对最低必要限度，并应遵守国家法律所确定、并由执法当局本身在每一具体紧急使用案例中规定的适当保障措施和条件。此外，在此类情形中，执法当局应在没有不当延迟的情况下且最迟在24小时内请求此类授权，同时说明未能更早请求的理由。如果此类授权被拒绝，与该授权相关的实时生物特征识别系统的使用应立即停止，与此类使用相关的所有数据应被丢弃和删除。此类数据包括

(18) 2002年6月13日关于欧洲逮捕令及成员国间移交程序的理事会框架决定2002/584/JHA(OJ L 190, 18.7.2002, p.1)。

(19) 欧洲议会和理事会 2022 年 12 月 14 日关于关键实体韧性并废止理事会 Directive 2008/114/EC 的 Directive (EU) 2022/2557(OJ L 333, 2

input data directly acquired by an AI system in the course of the use of such system as well as the results and outputs of the use linked to that authorisation. It should not include input that is legally acquired in accordance with another Union or national law. In any case, no decision producing an adverse legal effect on a person should be taken based solely on the output of the remote biometric identification system.

(36) In order to carry out their tasks in accordance with the requirements set out in this Regulation as well as in national rules, the relevant market surveillance authority and the national data protection authority should be notified of each use of the real-time biometric identification system. Market surveillance authorities and the national data protection authorities that have been notified should submit to the Commission an annual report on the use of real-time biometric identification systems.

(37) Furthermore, it is appropriate to provide, within the exhaustive framework set by this Regulation that such use in the territory of a Member State in accordance with this Regulation should only be possible where and in as far as the Member State concerned has decided to expressly provide for the possibility to authorise such use in its detailed rules of national law. Consequently, Member States remain free under this Regulation not to provide for such a possibility at all or to only provide for such a possibility in respect of some of the objectives capable of justifying authorised use identified in this Regulation. Such national rules should be notified to the Commission within 30 days of their adoption.

(38) The use of AI systems for real-time remote biometric identification of natural persons in publicly accessible spaces for the purpose of law enforcement necessarily involves the processing of biometric data. The rules of this Regulation that prohibit, subject to certain exceptions, such use, which are based on Article 16 TFEU, should apply as *lex specialis* in respect of the rules on the processing of biometric data contained in Article 10 of Directive (EU) 2016/680, thus regulating such use and the processing of biometric data involved in an exhaustive manner. Therefore, such use and processing should be possible only in as far as it is compatible with the framework set by this Regulation, without there being scope, outside that framework, for the competent authorities, where they act for purpose of law enforcement, to use such systems and process such data in connection thereto on the grounds listed in Article 10 of Directive (EU) 2016/680. In that context, this Regulation is not intended to provide the legal basis for the processing of personal data under Article 8 of Directive (EU) 2016/680. However, the use of real-time remote biometric identification systems in publicly accessible spaces for purposes other than law enforcement, including by competent authorities, should not be covered by the specific framework regarding such use for the purpose of law enforcement set by this Regulation. Such use for purposes other than law enforcement should therefore not be subject to the requirement of an authorisation under this Regulation and the applicable detailed rules of national law that may give effect to that authorisation.

(39) Any processing of biometric data and other personal data involved in the use of AI systems for biometric identification, other than in connection to the use of real-time remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement as regulated by this Regulation, should continue to comply with all requirements resulting from Article 10 of Directive (EU) 2016/680. For purposes other than law enforcement, Article 9(1) of Regulation (EU) 2016/679 and Article 10(1) of Regulation (EU) 2018/1725 prohibit the processing of biometric data subject to limited exceptions as provided in those Articles. In the application of Article 9(1) of Regulation (EU) 2016/679, the use of remote biometric identification for purposes other than law enforcement has already been subject to prohibition decisions by national data protection authorities.

(40) In accordance with Article 6a of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, as annexed to the TEU and to the TFEU, Ireland is not bound by the rules laid down in Article 5(1), first subparagraph, point (g), to the extent it applies to the use of biometric categorisation systems for activities in the field of police cooperation and judicial cooperation in criminal matters, Article 5(1), first subparagraph, point (d), to the extent it applies to the use of AI systems covered by that provision, Article 5(1), first subparagraph, point (h), Article 5(2) to (6) and Article 26(10) of this Regulation adopted on the basis of Article 16 TFEU which relate to the processing of personal data by the Member States when carrying out activities falling within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the TFEU, where Ireland is not bound by the rules governing the forms of judicial cooperation in criminal matters or police cooperation which require compliance with the provisions laid down on the basis of Article 16 TFEU.

(41) In accordance with Articles 2 and 2a of Protocol No 22 on the position of Denmark, annexed to the TEU and to the TFEU, Denmark is not bound by rules laid down in Article 5(1), first subparagraph, point (g), to the extent it applies to the use of biometric categorisation systems for activities in the field of police cooperation and judicial cooperation in criminal matters, Article 5(1), first subparagraph, point (d), to the extent it applies to the use of AI systems covered by that provision, Article 5(1), first subparagraph, point (h), (2) to (6) and Article 26(10) of this Regulation

人工智能系统在使用过程中直接获取的输入数据以及与该授权相关的使用结果和输出。它不应包括根据另一 Union 或国家法律合法获取的输入。在任何情况下，不得仅基于远程生物特征识别系统的输出作出对个人产生不利法律影响的决定。

(36) 为依照本条例及国家规则所规定的要求履行其任务，相关市场监督机构和国家数据保护机构应被告知每次使用实时生物特征识别系统的情况。已获通知的市场监督机构和国家数据保护机构应向委员会提交关于实时生物特征识别系统使用情况的年度报告。

(37) 此外，宜在本 Regulation 所设定的穷尽框架内规定，在

依照本条例在一成员国领土内进行，仅在该相关成员国已决定在其国家法详细规则中明确规定了授权此类使用的可能性时，且仅在此范围内，方为可能。因此，根据本条例，成员国仍可自由选择完全不规定此种可能性，或仅针对本条例所确定的、可为授权使用提供正当理由的部分目标规定此种可能性。此类国家规则应在其通过后30天内通知委员会。

(38) 为执法目的在可公开访问的空间对自然人使用人工智能系统进行实时远程生物特征识别必然涉及生物特征数据的处理。本 Regulation 中禁止此类使用（除某些例外情形外）的规则以《欧盟运行条约》第16条为基础，应作为特别法适用于 Directive (EU) 2016/680 第10条所载关于生物特征数据处理的规则，从而以穷尽的方式规范此类使用及所涉生物特征数据的处理。因此，此类使用和处理应仅在符合本 Regulation 所设框架的范围内才被允许，在该框架之外，主管机关在为执法目的行事时，不得以 Directive (EU) 2016/680 第10条所列理由使用此类系统并处理与此相关的此类数据。在此背景下，本 Regulation 无意提供 Directive (EU) 2016/680 第8条下个人数据处理的法律依据。然而，在可公开访问的空间为执法以外的目的（包括由主管机关）使用实时远程生物特征识别系统，不应被本 Regulation 所设关于此类为执法目的使用的特定框架所涵盖。因此，此类为执法以外目的的使用不应受本 Regulation 下授权要求以及可能使该授权生效的可适用国内法详细规则的约束。

(39) 在使用人工智能系统进行生物特征识别过程中涉及的任何生物特征数据和其他个人数据的处理

除与本条例所规范的为执法目的在可公开访问的空间使用实时远程生物特征识别系统相关的情形外，识别应继续遵守 (EU) 2016/680指令第10条产生的所有要求。对于执法以外的目的，(EU) 2016/679条例第9(1)条和(EU) 2018/1725条例第10(1)条禁止处理生物特征数据，但受这些条款所规定的有限例外约束。在适用(EU) 2016/679条例第9(1)条时，为执法以外目的使用远程生物特征识别已受到国家数据保护机构的禁止决定约束。

(40) 根据关于联合王国和爱尔兰在……方面立场的第21号议定书第6a条，

自由、安全与司法区域(附于《欧盟条约》和《欧盟运行条约》)，爱尔兰不受第5(1)条第一项第(g)点所规定规则的约束，在其适用于为警务合作和刑事事项司法合作领域活动使用生物特征分类系统的范围内；不受第5(1)条第一项第(d)点所规定规则的约束，在其适用于该条款所涵盖的人工智能系统使用的范围内；不受第5(1)条第一项第(h)点、第5(2)至(6)条以及第26(10)条的约束，这些条款系基于《欧盟运行条约》第16条通过，涉及成员国在开展属于《欧盟运行条约》第三部分第五编第4章或第5章范围内的活动时对个人数据的处理，而爱尔兰不受管辖刑事事项司法合作或警务合作形式的规则约束，该等规则要求遵守基于《欧盟运行条约》第16条所规定的条款。

(41) 根据附于TEU和……的关于丹麦立场的第22号议定书第2条和第2a条，

《欧盟运行条约》规定，丹麦不受本条例第5条第1款第一项(g)目所定规则的约束（就该目适用于警务合作及刑事司法合作领域活动中生物特征分类系统的使用而言），亦不受第5条第1款第一项(d)目（就该目适用于该条款所涵盖的人工智能系统的使用而言）、第5条第1款第一项(h)目、第(2)至(6)项及第26条第10款所定规则的约束

adopted on the basis of Article 16 TFEU, or subject to their application, which relate to the processing of personal data by the Member States when carrying out activities falling within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the TFEU.

(42) In line with the presumption of innocence, natural persons in the Union should always be judged on their actual behaviour. Natural persons should never be judged on AI-predicted behaviour based solely on their profiling, personality traits or characteristics, such as nationality, place of birth, place of residence, number of children, level of debt or type of car, without a reasonable suspicion of that person being involved in a criminal activity based on objective verifiable facts and without human assessment thereof. Therefore, risk assessments carried out with regard to natural persons in order to assess the likelihood of their offending or to predict the occurrence of an actual or potential criminal offence based solely on profiling them or on assessing their personality traits and characteristics should be prohibited. In any case, that prohibition does not refer to or touch upon risk analytics that are not based on the profiling of individuals or on the personality traits and characteristics of individuals, such as AI systems using risk analytics to assess the likelihood of financial fraud by undertakings on the basis of suspicious transactions or risk analytic tools to predict the likelihood of the localisation of narcotics or illicit goods by customs authorities, for example on the basis of known trafficking routes.

(43) The placing on the market, the putting into service for that specific purpose, or the use of AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage, should be prohibited because that practice adds to the feeling of mass surveillance and can lead to gross violations of fundamental rights, including the right to privacy.

(44) There are serious concerns about the scientific basis of AI systems aiming to identify or infer emotions, particularly as expression of emotions vary considerably across cultures and situations, and even within a single individual. Among the key shortcomings of such systems are the limited reliability, the lack of specificity and the limited generalisability. Therefore, AI systems identifying or inferring emotions or intentions of natural persons on the basis of their biometric data may lead to discriminatory outcomes and can be intrusive to the rights and freedoms of the concerned persons. Considering the imbalance of power in the context of work or education, combined with the intrusive nature of these systems, such systems could lead to detrimental or unfavourable treatment of certain natural persons or whole groups thereof. Therefore, the placing on the market, the putting into service, or the use of AI systems intended to be used to detect the emotional state of individuals in situations related to the workplace and education should be prohibited. That prohibition should not cover AI systems placed on the market strictly for medical or safety reasons, such as systems intended for therapeutical use.

(45) Practices that are prohibited by Union law, including data protection law, non-discrimination law, consumer protection law, and competition law, should not be affected by this Regulation.

(46) High-risk AI systems should only be placed on the Union market, put into service or used if they comply with certain mandatory requirements. Those requirements should ensure that high-risk AI systems available in the Union or whose output is otherwise used in the Union do not pose unacceptable risks to important Union public interests as recognised and protected by Union law. On the basis of the New Legislative Framework, as clarified in the Commission notice 'The "Blue Guide" on the implementation of EU product rules 2022' ([20]), the general rule is that more than one legal act of Union harmonisation legislation, such as Regulations (EU) 2017/745 ([21]) and (EU) 2017/746 ([22]) of the European Parliament and of the Council or Directive 2006/42/EC of the European Parliament and of the Council ([23]), may be applicable to one product, since the making available or putting into service can take

([20]) OJ C 247, 29.6.2022, p. 1.
([21]) Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117, 5.5.2017, p. 1).
([22]) Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on *in vitro* diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (OJ L 117, 5.5.2017, p. 176).
([23]) Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (OJ L 157, 9.6.2006, p. 24).

依据Article 16 TFEU通过，或受其适用约束，涉及成员国在开展属于TFEU第三部分第五章第4章或第5章范围内的活动时处理个人数据。

(42) 根据无罪推定原则，联盟内的自然人应始终根据其实际行为。不得仅凭对自然人的画像分析、人格特质或特征(如国籍、出生地、居住地、子女数量、负债水平或汽车类型)而基于人工智能预测的行为对自然人作出评判，除非有基于客观可核实事实的合理怀疑认为该人参与犯罪活动，且未经人工评估。因此，为评估自然人犯罪可能性或仅基于对其画像分析或评估其人格特质和特征来预测实际或潜在刑事犯罪发生而进行的风险评估应当被禁止。在任何情况下，该禁令不涉及也不触及并非基于个人画像分析或个人人格特质和特征的风险分析，例如利用风险分析评估企业基于可疑交易实施金融欺诈可能性的AI系统，或海关当局用于预测毒品或非法货物定位可能性的风险分析工具(例如基于已知贩运路线)。

(43) 投放市场、为特定目的投入使用或使用会创造或通过从互联网或CCTV录像中无针对性地抓取面部图像来扩展面部识别数据库的人工智能系统，应被禁止，因为这种做法加剧了大规模监控的感觉，并可能导致严重侵犯基本权利，包括隐私权。

(44) 对于旨在识别或推断情绪的人工智能系统的科学基础存在严重关切，特别是因为情绪的表达在不同文化和情境下差异很大，甚至在单个人内部也是如此。此类系统的主要缺陷包括可靠性有限、缺乏特异性和泛化能力有限。因此，基于生物识别数据识别或推断自然人情緒或意图的人工智能系统可能导致歧视性结果，并可能侵犯相关人员的权利和自由。考虑到工作或教育背景下的权力不平衡，加之这些系统的侵入性，此类系统可能导致某些自然人或整个群体受到有害或不利的待遇。因此，旨在用于在工作场所和教育相关情境中检测个人情绪状态的人工智能系统的投放市场、投入使用或使用应当被禁止。该禁令不应涵盖严格出于医疗或安全原因投放市场的人工智能系统，例如用于治疗目的的系统。

(45) 被Union law禁止的做法，包括数据保护法、非歧视法、消费者保护法及竞争法不应受本条例影响。

(46) 高风险人工智能系统只有在符合以下条件时，才应投放联盟市场、投入使用或使用：某些强制性要求。这些要求应确保在欧盟境内可用或其输出以其他方式在欧盟境内使用的高风险人工智能系统不会对欧盟法律所承认和保护的欧盟重要公共利益构成不可接受的风险。根据新立法框架，正如委员会通知《关于实施2022年欧盟产品规则的"蓝皮书"》(20)所澄清的，一般规则是，不止一项欧盟协调立法法案，例如欧洲议会和理事会的(EU) 2017/745号条例(21)和(EU) 2017/746号条例(22)或欧洲议会和理事会的2006/42/EC号指令(23)，可能适用于同一产品，因为只有在产品符合所有适用的欧盟协调立法时才能提供或投入使用。

(20) OJ C 247, 29.6.2022， 第1页。
(21) 欧洲议会和理事会2017年4月5日关于医疗器械的条例(EU) 2017/745，修订指令2001/83/EC、条例(EC) No 178/2002和条例(EC) No 1223/2009，并废止理事会指令90/385/EEC和93/42/EEC(OJ L 117, 5.5.2017, p.1)。
(22) 欧洲议会和理事会2017年4月5日关于体外诊断医疗器械并废止指令98/79/EC及委员会决定2010/227/EU的(EU) 2017/746号条例(OJ L 117, 5.5.2017, p.176)。
(23) 欧洲议会和理事会2006年5月17日关于机械的指令2006/42/EC，并修订指令95/16/EC(OJ L 157, 9.6.2006, p.24)。

place only when the product complies with all applicable Union harmonisation legislation. To ensure consistency and avoid unnecessary administrative burdens or costs, providers of a product that contains one or more high-risk AI systems, to which the requirements of this Regulation and of the Union harmonisation legislation listed in an annex to this Regulation apply, should have flexibility with regard to operational decisions on how to ensure compliance of a product that contains one or more AI systems with all applicable requirements of the Union harmonisation legislation in an optimal manner. AI systems identified as high-risk should be limited to those that have a significant harmful impact on the health, safety and fundamental rights of persons in the Union and such limitation should minimise any potential restriction to international trade.

(47) AI systems could have an adverse impact on the health and safety of persons, in particular when such systems operate as safety components of products. Consistent with the objectives of Union harmonisation legislation to facilitate the free movement of products in the internal market and to ensure that only safe and otherwise compliant products find their way into the market, it is important that the safety risks that may be generated by a product as a whole due to its digital components, including AI systems, are duly prevented and mitigated. For instance, increasingly autonomous robots, whether in the context of manufacturing or personal assistance and care should be able to safely operate and performs their functions in complex environments. Similarly, in the health sector where the stakes for life and health are particularly high, increasingly sophisticated diagnostics systems and systems supporting human decisions should be reliable and accurate.

(48) The extent of the adverse impact caused by the AI system on the fundamental rights protected by the Charter is of particular relevance when classifying an AI system as high risk. Those rights include the right to human dignity, respect for private and family life, protection of personal data, freedom of expression and information, freedom of assembly and of association, the right to non-discrimination, the right to education, consumer protection, workers' rights, the rights of persons with disabilities, gender equality, intellectual property rights, the right to an effective remedy and to a fair trial, the right of defence and the presumption of innocence, and the right to good administration. In addition to those rights, it is important to highlight the fact that children have specific rights as enshrined in Article 24 of the Charter and in the United Nations Convention on the Rights of the Child, further developed in the UNCRC General Comment No 25 as regards the digital environment, both of which require consideration of the children's vulnerabilities and provision of such protection and care as necessary for their well-being. The fundamental right to a high level of environmental protection enshrined in the Charter and implemented in Union policies should also be considered when assessing the severity of the harm that an AI system can cause, including in relation to the health and safety of persons.

(49) As regards high-risk AI systems that are safety components of products or systems, or which are themselves products or systems falling within the scope of Regulation (EC) No 300/2008 of the European Parliament and of the Council ([24]), Regulation (EU) No 167/2013 of the European Parliament and of the Council ([25]), Regulation (EU) No 168/2013 of the European Parliament and of the Council ([26]), Directive 2014/90/EU of the European Parliament and of the Council ([27]), Directive (EU) 2016/797 of the European Parliament and of the Council ([28]), Regulation (EU) 2018/858 of the European Parliament and of the Council ([29]), Regulation (EU) 2018/1139 of the

([24]) Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (OJ L 97, 9.4.2008, p. 72).

([25]) Regulation (EU) No 167/2013 of the European Parliament and of the Council of 5 February 2013 on the approval and market surveillance of agricultural and forestry vehicles (OJ L 60, 2.3.2013, p. 1).

([26]) Regulation (EU) No 168/2013 of the European Parliament and of the Council of 15 January 2013 on the approval and market surveillance of two- or three-wheel vehicles and quadricycles (OJ L 60, 2.3.2013, p. 52).

([27]) Directive 2014/90/EU of the European Parliament and of the Council of 23 July 2014 on marine equipment and repealing Council Directive 96/98/EC (OJ L 257, 28.8.2014, p. 146).

([28]) Directive (EU) 2016/797 of the European Parliament and of the Council of 11 May 2016 on the interoperability of the rail system within the European Union (OJ L 138, 26.5.2016, p. 44).

([29]) Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC (OJ L 151, 14.6.2018, p. 1).

只有在产品符合所有适用的欧盟协调立法时才能提供或投入使用。为确保一致性并避免不必要的行政负担或成本，对于包含一个或多个高风险人工智能系统且本 Regulation 的要求与本 Regulation 附件所列欧盟协调立法均适用的产品，其提供者应在如何以最佳方式确保包含一个或多个人工智能系统的产品符合欧盟协调立法所有适用要求的运营决策方面具有灵活性。被认定为高风险的人工智能系统应限于那些对欧盟境内人员的健康、安全和基本权利产生重大有害影响的系统，此种限制应尽量减少对国际贸易的任何潜在限制。

(47) 人工智能系统可能对人员的健康和安全产生不利影响，特别是当此类系统作为产品的安全组件运行时。与欧盟协调立法促进产品在内部市场自由流通并确保只有安全且在其他方面合规的产品进入市场的目标相一致，重要的是，产品整体因其数字组件(包括人工智能系统)可能产生的安全风险应得到适当预防和缓解。例如，日益自主的机器人，无论是在制造还是个人协助和护理背景下，都应能够在复杂环境中安全运行并执行其功能。同样，在生命和健康风险特别高的卫生领域，日益复杂的诊断系统和辅助人类决策的系统应可靠且准确。

(48) 人工智能系统对《宪章》所保护基本权利造成的不利影响的程度具有

在将人工智能系统归类为高风险时，这些权利尤其相关。这些权利包括人的尊严权、尊重私人和家庭生活权、个人数据保护权、表达和信息自由权、集会和结社自由权、不受歧视权、受教育权、消费者保护、工人权利、残疾人权利、性别平等、知识产权、获得有效补救和公正审判的权利、辩护权和无罪推定，以及良好行政权。除这些权利外，还必须强调，儿童享有《宪章》第24条和《联合国儿童权利公约》所规定的特定权利，联合国儿童权利委员会第25号一般性意见就数字环境进一步阐述了这些权利，这两项文书都要求考虑儿童的脆弱性，并为其福祉提供必要的保护和照料。《宪章》所规定并在欧盟政策中实施的享有高水平环境保护的基本权利，在评估人工智能系统可能造成的损害的严重性时也应予以考虑，包括与人员健康和安全有关的损害。

(49) 关于作为产品或系统安全组件的高风险人工智能系统，或本身即为

属于欧洲议会和理事会第(EC) No 300/2008号条例(24)、欧洲议会和理事会第(EU) No 167/2013号条例(25)、欧洲议会和理事会第(EU) No 168/2013号条例(26)、欧洲议会和理事会第2014/90/EU号指令(27)、欧洲议会和理事会第(EU) 2016/797号指令(28)、欧洲议会和理事会第(EU) 2018/858号条例(29)、第(EU) 2018/1139号条例

(24) 欧洲议会和理事会2008年3月11日关于民用航空安保领域共同规则并废止(EC) No 2320/2002号条例的(EC) No 300/2008号条例(OJ L 97, 9.4.2008, p.72)。

(25) 欧洲议会和理事会2013年2月5日关于农林车辆批准和市场监督的第(EU)167/2013号条例(OJ L 60, 2.3.2013, p.1)。

(26) 欧洲议会和理事会2013年1月15日关于两轮或三轮车辆和四轮车批准与市场监督的(EU)第168/2013号条例(OJ L 60, 2.3.2013, p.52)。

(27) 欧洲议会和理事会2014年7月23日关于船用设备并废除理事会第96/98/EC号指令的第2014/90/EU号指令(OJ L 257, 28.8.2014, p.146)。

(28) 欧洲议会和理事会2016年5月11日关于欧盟内部铁路系统互操作性的指令(EU) 2016/797(OJ L 138,2016年5月26日，第44页)。

(29) 欧洲议会和理事会2018年5月30日关于机动车及其挂车以及用于此类车辆的系统、部件和独立技术单元的型式认证和市场监督，修订条例(EC) No 715/2007和(EC) No 595/2009并废止指令2007/46/EC的条例(EU) 2018/858(OJ L 151, 14.6.2018, p.1)。

European Parliament and of the Council ([30]), and Regulation (EU) 2019/2144 of the European Parliament and of the Council ([31]), it is appropriate to amend those acts to ensure that the Commission takes into account, on the basis of the technical and regulatory specificities of each sector, and without interfering with existing governance, conformity assessment and enforcement mechanisms and authorities established therein, the mandatory requirements for high-risk AI systems laid down in this Regulation when adopting any relevant delegated or implementing acts on the basis of those acts.

(50) As regards AI systems that are safety components of products, or which are themselves products, falling within the scope of certain Union harmonisation legislation listed in an annex to this Regulation, it is appropriate to classify them as high-risk under this Regulation if the product concerned undergoes the conformity assessment procedure with a third-party conformity assessment body pursuant to that relevant Union harmonisation legislation. In particular, such products are machinery, toys, lifts, equipment and protective systems intended for use in potentially explosive atmospheres, radio equipment, pressure equipment, recreational craft equipment, cableway installations, appliances burning gaseous fuels, medical devices, *in vitro* diagnostic medical devices, automotive and aviation.

(51) The classification of an AI system as high-risk pursuant to this Regulation should not necessarily mean that the product whose safety component is the AI system, or the AI system itself as a product, is considered to be high-risk under the criteria established in the relevant Union harmonisation legislation that applies to the product. This is, in particular, the case for Regulations (EU) 2017/745 and (EU) 2017/746, where a third-party conformity assessment is provided for medium-risk and high-risk products.

(52) As regards stand-alone AI systems, namely high-risk AI systems other than those that are safety components of products, or that are themselves products, it is appropriate to classify them as high-risk if, in light of their intended purpose, they pose a high risk of harm to the health and safety or the fundamental rights of persons, taking into account both the severity of the possible harm and its probability of occurrence and they are used in a number of specifically pre-defined areas specified in this Regulation. The identification of those systems is based on the same methodology and criteria envisaged also for any future amendments of the list of high-risk AI systems that the Commission should be empowered to adopt, via delegated acts, to take into account the rapid pace of technological development, as well as the potential changes in the use of AI systems.

(53) It is also important to clarify that there may be specific cases in which AI systems referred to in pre-defined areas specified in this Regulation do not lead to a significant risk of harm to the legal interests protected under those areas because they do not materially influence the decision-making or do not harm those interests substantially. For the purposes of this Regulation, an AI system that does not materially influence the outcome of decision-making should be understood to be an AI system that does not have an impact on the substance, and thereby the outcome, of decision-making, whether human or automated. An AI system that does not materially influence the outcome of decision-making could include situations in which one or more of the following conditions are fulfilled. The first such condition should be that the AI system is intended to perform a narrow procedural task, such as an AI system that transforms unstructured data into structured data, an AI system that classifies incoming documents into categories or an AI system that is used to detect duplicates among a large number of applications. Those tasks are of such narrow and limited nature that they pose only limited risks which are not increased through the use of an AI system in a context that is listed as a high-risk use in an annex to this Regulation. The second condition should be

([30]) Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (OJ L 212, 22.8.2018, p. 1).

([31]) Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166 (OJ L 325, 16.12.2019, p. 1).

(30)以及欧洲议会和理事会第(EU) 2019/2144号条例(31)范围内的产品或系统，宜修订这些法案，以确保委员会在根据这些法案通过任何相关授权法案或实施法案时，基于各部门的技术和监管特殊性，且不干扰其中既有的治理、合格评定和执行机制及机构，考虑本条例规定的高风险人工智能系统的强制性要求。

(50) 对于属于产品安全组件的人工智能系统，或本身即为属于本条例附件所列某些欧盟协调立法范围内的产品的人工智能系统，如果有关产品依据相关欧盟协调立法接受第三方合格评定机构的合格评定程序，则宜将其归类为本条例下的高风险系统。此类产品尤其包括机械、玩具、电梯、用于潜在爆炸性环境的设备和防护系统、无线电设备、压力设备、游艇设备、索道装置、燃气燃烧器具、医疗器械、体外诊断医疗器械、汽车和航空。

(51) 依据本Regulation将人工智能系统归类为高风险，不一定意味着

其安全组件为该人工智能系统的产品，或作为产品的人工智能系统本身，根据适用于该产品的相关Union harmonisation legislation所确立的标准被视为高风险。尤其是Regulations(EU) 2017/745和(EU) 2017/746的情况，其中为中等风险和高风险产品规定了第三方合格评定。

(52) 关于独立人工智能系统，即除作为安全组件的高风险人工智能系统以外的高风险人工智能系统

产品或本身即为产品的人工智能系统，如果根据其预期用途，对人员的健康和安全或基本权利构成高损害风险，同时考虑到可能损害的严重性及其发生概率，并且它们被用于本条例规定的若干具体预先界定的领域，则宜将其归类为高风险。对这些系统的识别基于与委员会应有权通过授权法案对未来高风险人工智能系统清单进行的任何修订所设想的相同方法和标准，以考虑到技术发展的快速步伐以及人工智能系统使用方面的潜在变化。

(53) 同样重要的是澄清，可能存在特定情形，其中在预先定义领域提及的人工智能系统

本条例规定的.....不会对上述领域所保护的法益造成重大损害风险，因为它们不会实质性影响决策，也不会实质性损害这些法益。就本条例而言，不实质性影响决策结果的人工智能系统应被理解为不对决策(无论是人工决策还是自动化决策)的实质内容、进而不对决策结果产生影响的人工智能系统。不实质性影响决策结果的人工智能系统可包括满足以下一项或多项条件的情形。第一个此类条件应为：该人工智能系统旨在执行狭窄的程序性任务，例如将非结构化数据转换为结构化数据的人工智能系统、将来文文件分类归入各类别的人工智能系统，或用于在大量申请中检测重复项的人工智能系统。这些任务的性质如此狭窄和有限，以致其仅带来有限风险，且在本条例附件所列高风险使用场景中使用人工智能系统并不会增加该等风险。第二个条件应为

(30) 欧洲议会和理事会2018年7月4日关于民用航空领域共同规则并设立欧盟航空安全局、修订欧洲议会和理事会第(EC) No 2111/2005号条例、第(EC) No 1008/2008号条例、第(EU) No 996/2010号条例、第(EU) No 376/2014号条例及第2014/30/EU号和第2014/53/EU号指令、并废止欧洲议会和理事会第(EC) No 552/2004号条例和第(EC) No 216/2008号条例及理事会第(EEC) No 3922/91号条例的第(EU) 2018/1139号条例(OJ L 212, 22.8.2018， 第1页)。

(31) 欧洲议会和理事会2019年11月27日关于机动车及其挂车以及用于此类车辆的系统、部件和独立技术单元在一般安全性和车辆乘员及弱势道路使用者保护方面的型式认证要求的条例(EU) 2019/2144，修订欧洲议会和理事会条例(EU) 2018/858并废止欧洲议会和理事会条例(EC)第78/2009号、(EC)第79/2009号和(EC)第661/2009号以及委员会条例(EC)第631/2009号、(EU)第406/2010号、(EU)第672/2010号、(EU)第1003/2010号、(EU)第1005/2010号、(EU)第1008/2010号、(EU)第1009/2010号、(EU)第19/2011号、(EU)第109/2011号、(EU)第458/2011号、(EU)第65/2012号、(EU)第130/2012号、(EU)第347/2012号、(EU)第351/2012号、(EU)第1230/2012号和(EU) 2015/166号（OJ L 325，2019年12月16日，第1页）。

that the task performed by the AI system is intended to improve the result of a previously completed human activity that may be relevant for the purposes of the high-risk uses listed in an annex to this Regulation. Considering those characteristics, the AI system provides only an additional layer to a human activity with consequently lowered risk. That condition would, for example, apply to AI systems that are intended to improve the language used in previously drafted documents, for example in relation to professional tone, academic style of language or by aligning text to a certain brand messaging. The third condition should be that the AI system is intended to detect decision-making patterns or deviations from prior decision-making patterns. The risk would be lowered because the use of the AI system follows a previously completed human assessment which it is not meant to replace or influence, without proper human review. Such AI systems include for instance those that, given a certain grading pattern of a teacher, can be used to check *ex post* whether the teacher may have deviated from the grading pattern so as to flag potential inconsistencies or anomalies. The fourth condition should be that the AI system is intended to perform a task that is only preparatory to an assessment relevant for the purposes of the AI systems listed in an annex to this Regulation, thus making the possible impact of the output of the system very low in terms of representing a risk for the assessment to follow. That condition covers, inter alia, smart solutions for file handling, which include various functions from indexing, searching, text and speech processing or linking data to other data sources, or AI systems used for translation of initial documents. In any case, AI systems used in high-risk use-cases listed in an annex to this Regulation should be considered to pose significant risks of harm to the health, safety or fundamental rights if the AI system implies profiling within the meaning of Article 4, point (4) of Regulation (EU) 2016/679 or Article 3, point (4) of Directive (EU) 2016/680 or Article 3, point (5) of Regulation (EU) 2018/1725. To ensure traceability and transparency, a provider who considers that an AI system is not high-risk on the basis of the conditions referred to above should draw up documentation of the assessment before that system is placed on the market or put into service and should provide that documentation to national competent authorities upon request. Such a provider should be obliged to register the AI system in the EU database established under this Regulation. With a view to providing further guidance for the practical implementation of the conditions under which the AI systems listed in an annex to this Regulation are, on an exceptional basis, non-high-risk, the Commission should, after consulting the Board, provide guidelines specifying that practical implementation, completed by a comprehensive list of practical examples of use cases of AI systems that are high-risk and use cases that are not.

(54) As biometric data constitutes a special category of personal data, it is appropriate to classify as high-risk several critical-use cases of biometric systems, insofar as their use is permitted under relevant Union and national law. Technical inaccuracies of AI systems intended for the remote biometric identification of natural persons can lead to biased results and entail discriminatory effects. The risk of such biased results and discriminatory effects is particularly relevant with regard to age, ethnicity, race, sex or disabilities. Remote biometric identification systems should therefore be classified as high-risk in view of the risks that they pose. Such a classification excludes AI systems intended to be used for biometric verification, including authentication, the sole purpose of which is to confirm that a specific natural person is who that person claims to be and to confirm the identity of a natural person for the sole purpose of having access to a service, unlocking a device or having secure access to premises. In addition, AI systems intended to be used for biometric categorisation according to sensitive attributes or characteristics protected under Article 9(1) of Regulation (EU) 2016/679 on the basis of biometric data, in so far as these are not prohibited under this Regulation, and emotion recognition systems that are not prohibited under this Regulation, should be classified as high-risk. Biometric systems which are intended to be used solely for the purpose of enabling cybersecurity and personal data protection measures should not be considered to be high-risk AI systems.

(55) As regards the management and operation of critical infrastructure, it is appropriate to classify as high-risk the AI systems intended to be used as safety components in the management and operation of critical digital infrastructure as listed in point (8) of the Annex to Directive (EU) 2022/2557, road traffic and the supply of water, gas, heating and electricity, since their failure or malfunctioning may put at risk the life and health of persons at large scale and lead to appreciable disruptions in the ordinary conduct of social and economic activities. Safety components of critical infrastructure, including critical digital infrastructure, are systems used to directly protect the physical integrity of critical infrastructure or the health and safety of persons and property but which are not necessary in order for the

人工智能系统所执行的任务旨在改进先前已完成的人类活动的结果，该结果可能与本 Regulation 附件所列高风险用途相关。考虑到这些特征，人工智能系统仅对人类活动提供附加层，因而风险较低。例如，该条件适用于旨在改进先前起草文件中所用语言的人工智能系统，例如在专业语气、学术语言风格方面，或通过使文本与特定品牌信息保持一致。第三个条件应是，人工智能系统旨在检测决策模式或对先前决策模式的偏离。风险将降低，因为人工智能系统的使用遵循先前已完成的人工评估，且在没有适当人工审查的情况下，该系统并非旨在取代或影响该评估。此类人工智能系统包括例如这样的系统：给定教师的特定评分模式，可用于事后检查教师是否可能偏离了评分模式，以标记潜在的不一致或异常。第四个条件应是，人工智能系统旨在执行的任务仅为本 Regulation 附件所列人工智能系统相关评估的准备性工作，从而使系统输出的可能影响在构成后续评估风险方面非常低。该条件尤其涵盖文件处理的智能解决方案，包括索引、搜索、文本和语音处理或将数据链接到其他数据源等各种功能，或用于翻译初始文件的人工智能系统。在任何情况下，如果人工智能系统意味着 Regulation (EU) 2016/679 第4条第(4)点、Directive (EU) 2016/680 第3条第(4)点或 Regulation (EU) 2018/1725 第3条第(5)点意义上的画像，则本 Regulation 附件所列高风险用例中使用的人工智能系统应被视为对健康、安全或基本权利构成重大损害风险。为确保可追溯性和透明度，认为人工智能系统基于上述条件不属于高风险的提供者，应在该系统投放市场或投入使用前起草评估文档，并应国家主管机关要求提供该文档。此类提供者有义务在本 Regulation 所建立的欧盟数据库中注册该人工智能系统。为就本 Regulation 附件所列人工智能系统在例外情况下非高风险的条件的实际实施提供进一步指导，委员会应在咨询委员会后提供指南，明确该实际实施，并辅以高风险用例和非高风险用例的人工智能系统实际示例的综合清单。

(54) 由于生物特征数据构成特殊类别的个人数据，宜将若干生物特征系统的关键用例，前提是其使用为相关欧盟法和国家法所允许。旨在对自然人进行远程生物特征识别的人工智能系统的技术不准确性可能导致有偏差的结果并产生歧视性影响。此类有偏差结果和歧视性影响的风险在年龄、族裔、种族、性别或残疾方面尤为相关。因此，鉴于其带来的风险，远程生物特征识别系统应被归类为高风险。此类分类不包括旨在用于生物特征验证(包括身份验证)的人工智能系统，其唯一目的是确认特定自然人确为其所声称之人，以及仅为访问服务、解锁设备或安全进入场所之目的而确认自然人身份。此外，旨在基于生物特征数据根据《(EU) 2016/679号条例》第9条第(1)条所保护的敏感属性或特征进行生物特征分类的人工智能系统(前提是此类系统未被本条例禁止)，以及未被本条例禁止的情绪识别系统，应被归类为高风险。仅旨在用于实现网络安全和个人数据保护措施的生物特征系统不应被视为高风险人工智能系统。

(55) 关于关键基础设施的管理和运营，宜将以下人工智能系统归类为高风险：旨在用作指令(EU) 2022/2557附件第(8)点所列关键数字基础设施、道路交通以及水、燃气、供暖和电力供应的管理和运营中的安全组件的系统，因为其故障或失灵可能大规模危及人的生命和健康，并对社会和经济活动的正常开展造成显著干扰。关键基础设施(包括关键数字基础设施)的安全组件是用于直接保护关键基础设施的物理完整性或人的健康与安全及财产的系统，但这些系统并非为

system to function. The failure or malfunctioning of such components might directly lead to risks to the physical integrity of critical infrastructure and thus to risks to health and safety of persons and property. Components intended to be used solely for cybersecurity purposes should not qualify as safety components. Examples of safety components of such critical infrastructure may include systems for monitoring water pressure or fire alarm controlling systems in cloud computing centres.

(56) The deployment of AI systems in education is important to promote high-quality digital education and training and to allow all learners and teachers to acquire and share the necessary digital skills and competences, including media literacy, and critical thinking, to take an active part in the economy, society, and in democratic processes. However, AI systems used in education or vocational training, in particular for determining access or admission, for assigning persons to educational and vocational training institutions or programmes at all levels, for evaluating learning outcomes of persons, for assessing the appropriate level of education for an individual and materially influencing the level of education and training that individuals will receive or will be able to access or for monitoring and detecting prohibited behaviour of students during tests should be classified as high-risk AI systems, since they may determine the educational and professional course of a person's life and therefore may affect that person's ability to secure a livelihood. When improperly designed and used, such systems may be particularly intrusive and may violate the right to education and training as well as the right not to be discriminated against and perpetuate historical patterns of discrimination, for example against women, certain age groups, persons with disabilities, or persons of certain racial or ethnic origins or sexual orientation.

(57) AI systems used in employment, workers management and access to self-employment, in particular for the recruitment and selection of persons, for making decisions affecting terms of the work-related relationship, promotion and termination of work-related contractual relationships, for allocating tasks on the basis of individual behaviour, personal traits or characteristics and for monitoring or evaluation of persons in work-related contractual relationships, should also be classified as high-risk, since those systems may have an appreciable impact on future career prospects, livelihoods of those persons and workers' rights. Relevant work-related contractual relationships should, in a meaningful manner, involve employees and persons providing services through platforms as referred to in the Commission Work Programme 2021. Throughout the recruitment process and in the evaluation, promotion, or retention of persons in work-related contractual relationships, such systems may perpetuate historical patterns of discrimination, for example against women, certain age groups, persons with disabilities, or persons of certain racial or ethnic origins or sexual orientation. AI systems used to monitor the performance and behaviour of such persons may also undermine their fundamental rights to data protection and privacy.

(58) Another area in which the use of AI systems deserves special consideration is the access to and enjoyment of certain essential private and public services and benefits necessary for people to fully participate in society or to improve one's standard of living. In particular, natural persons applying for or receiving essential public assistance benefits and services from public authorities namely healthcare services, social security benefits, social services providing protection in cases such as maternity, illness, industrial accidents, dependency or old age and loss of employment and social and housing assistance, are typically dependent on those benefits and services and in a vulnerable position in relation to the responsible authorities. If AI systems are used for determining whether such benefits and services should be granted, denied, reduced, revoked or reclaimed by authorities, including whether beneficiaries are legitimately entitled to such benefits or services, those systems may have a significant impact on persons' livelihood and may infringe their fundamental rights, such as the right to social protection, non-discrimination, human dignity or an effective remedy and should therefore be classified as high-risk. Nonetheless, this Regulation should not hamper the development and use of innovative approaches in the public administration, which would stand to benefit from a wider use of compliant and safe AI systems, provided that those systems do not entail a high risk to legal and natural persons. In addition, AI systems used to evaluate the credit score or creditworthiness of natural persons should be classified as high-risk AI systems, since they determine those persons' access to financial resources or essential services such as housing, electricity, and telecommunication services. AI systems used for those purposes may lead to discrimination between persons or groups and may perpetuate historical patterns of discrimination, such as that based on racial or ethnic origins, gender, disabilities, age or sexual orientation, or may create new forms of discriminatory impacts. However, AI systems provided for by Union law for the purpose of detecting fraud in the offering of financial services and for prudential purposes to calculate credit institutions' and insurance undertakings' capital requirements should not be considered to be high-risk under this Regulation. Moreover, AI systems intended

系统运行。此类组件的故障或失灵可能直接导致关键基础设施物理完整性的风险，从而对人员健康和财产安全构成风险。仅用于网络安全目的的组件不应被视为安全组件。此类关键基础设施安全组件的示例可能包括用于监测水压的系统或云计算中心中的火灾报警控制系统。

(56) 在教育中部署人工智能系统对于促进高质量数字教育和培训十分重要，并且使所有学习者和教师能够获得和分享必要的数字技能和能力(包括媒体素养)以及批判性思维，从而积极参与经济、社会和民主进程。然而，用于教育或职业培训的人工智能系统，特别是用于确定入学或录取、将人员分配到各级教育和职业培训机构或项目、评估人员的学习成果、评估个人适当的教育水平并实质性影响个人将接受或能够获得的教育和培训水平，或用于在考试期间监测和检测学生被禁止的行为的系统，应被归类为高风险人工智能系统，因为它们可能决定一个人一生的教育和职业道路，从而可能影响该人谋生的能力。此类系统如果设计和使用不当，可能具有特别的侵入性，可能侵犯受教育和培训的权利以及不受歧视的权利，并延续历史上的歧视模式，例如对妇女、某些年龄群体、残疾人或某些种族或族裔出身或性取向的人的歧视。

(57) 用于就业、工人管理和自营职业准入的人工智能系统，特别是用于人员的招聘和选拔，用于作出影响工作相关关系条款、工作相关合同关系的晋升和终止的决定，用于根据个人行为、个人特质或特征分配任务，以及用于监测或评估处于工作相关合同关系中的人员的系统，也应被归类为高风险，因为这些系统可能对未来职业前景、这些人的生计和劳动者权利产生显著影响。相关的工作相关合同关系应以有意义的方式涉及雇员和通过2021年委员会工作计划所述平台提供服务的人员。在整个招聘过程中以及在评估、晋升或留用处于工作相关合同关系中的人员时，此类系统可能延续历史上的歧视模式，例如对妇女、某些年龄群体、残疾人或某些种族或族裔出身或性取向的人的歧视。用于监测此类人员绩效和行为的人工智能系统还可能损害其数据保护和隐私的基本权利。

(58) 使用人工智能系统值得特别考虑的另一个领域是获取和享有某些必要的私人和公共服务及福利，这些服务及福利是人们充分参与社会或提高生活水平所必需的。特别是，向公共当局申请或接受基本公共援助福利和服务的自然人，即医疗保健服务、社会保障福利、在生育、疾病、工伤、依赖或年老以及失业等情况下提供保护的社会服务以及社会和住房援助，通常依赖这些福利和服务，并相对于主管当局处于弱势地位。如果人工智能系统被用于确定当局是否应给予、拒绝、减少、撤销或收回此类福利和服务，包括受益人是否有合法资格获得此类福利或服务，这些系统可能对人们的生计产生重大影响，并可能侵犯其基本权利，例如社会保护权、不受歧视权、人的尊严权或获得有效补救的权利，因此应被归类为高风险。尽管如此，本条例不应妨碍公共行政部门开发和采用创新方法，这些方法将从更广泛地使用合规和安全的人工智能系统中受益，前提是这些系统不会对法人和自然人构成高风险。此外，用于评估自然人信用评分或信用worthiness的人工智能系统应被归类为高风险人工智能系统，因为它们决定了这些人获得金融资源或住房、电力和电信服务等基本服务的机会。用于这些目的的人工智能系统可能导致个人或群体之间的歧视，并可能延续历史上的歧视模式，例如基于种族或族裔出身、性别、残疾、年龄或性取向的歧视，或可能产生新形式的歧视性影响。然而，联盟法律为发现金融服务提供中的欺诈目的以及为审慎目的计算信贷机构和保险 undertaking 的资本要求而规定的人工智能系统，不应被视为本条例下的高风险。此外，旨在

to be used for risk assessment and pricing in relation to natural persons for health and life insurance can also have a significant impact on persons' livelihood and if not duly designed, developed and used, can infringe their fundamental rights and can lead to serious consequences for people's life and health, including financial exclusion and discrimination. Finally, AI systems used to evaluate and classify emergency calls by natural persons or to dispatch or establish priority in the dispatching of emergency first response services, including by police, firefighters and medical aid, as well as of emergency healthcare patient triage systems, should also be classified as high-risk since they make decisions in very critical situations for the life and health of persons and their property.

(59) Given their role and responsibility, actions by law enforcement authorities involving certain uses of AI systems are characterised by a significant degree of power imbalance and may lead to surveillance, arrest or deprivation of a natural person's liberty as well as other adverse impacts on fundamental rights guaranteed in the Charter. In particular, if the AI system is not trained with high-quality data, does not meet adequate requirements in terms of its performance, its accuracy or robustness, or is not properly designed and tested before being put on the market or otherwise put into service, it may single out people in a discriminatory or otherwise incorrect or unjust manner. Furthermore, the exercise of important procedural fundamental rights, such as the right to an effective remedy and to a fair trial as well as the right of defence and the presumption of innocence, could be hampered, in particular, where such AI systems are not sufficiently transparent, explainable and documented. It is therefore appropriate to classify as high-risk, insofar as their use is permitted under relevant Union and national law, a number of AI systems intended to be used in the law enforcement context where accuracy, reliability and transparency is particularly important to avoid adverse impacts, retain public trust and ensure accountability and effective redress. In view of the nature of the activities and the risks relating thereto, those high-risk AI systems should include in particular AI systems intended to be used by or on behalf of law enforcement authorities or by Union institutions, bodies, offices, or agencies in support of law enforcement authorities for assessing the risk of a natural person to become a victim of criminal offences, as polygraphs and similar tools, for the evaluation of the reliability of evidence in in the course of investigation or prosecution of criminal offences, and, insofar as not prohibited under this Regulation, for assessing the risk of a natural person offending or reoffending not solely on the basis of the profiling of natural persons or the assessment of personality traits and characteristics or the past criminal behaviour of natural persons or groups, for profiling in the course of detection, investigation or prosecution of criminal offences. AI systems specifically intended to be used for administrative proceedings by tax and customs authorities as well as by financial intelligence units carrying out administrative tasks analysing information pursuant to Union anti-money laundering law should not be classified as high-risk AI systems used by law enforcement authorities for the purpose of prevention, detection, investigation and prosecution of criminal offences. The use of AI tools by law enforcement and other relevant authorities should not become a factor of inequality, or exclusion. The impact of the use of AI tools on the defence rights of suspects should not be ignored, in particular the difficulty in obtaining meaningful information on the functioning of those systems and the resulting difficulty in challenging their results in court, in particular by natural persons under investigation.

(60) AI systems used in migration, asylum and border control management affect persons who are often in particularly vulnerable position and who are dependent on the outcome of the actions of the competent public authorities. The accuracy, non-discriminatory nature and transparency of the AI systems used in those contexts are therefore particularly important to guarantee respect for the fundamental rights of the affected persons, in particular their rights to free movement, non-discrimination, protection of private life and personal data, international protection and good administration. It is therefore appropriate to classify as high-risk, insofar as their use is permitted under relevant Union and national law, AI systems intended to be used by or on behalf of competent public authorities or by Union institutions, bodies, offices or agencies charged with tasks in the fields of migration, asylum and border control management as polygraphs and similar tools, for assessing certain risks posed by natural persons entering the territory of a Member State or applying for visa or asylum, for assisting competent public authorities for the examination, including related assessment of the reliability of evidence, of applications for asylum, visa and residence permits and associated complaints with regard to the objective to establish the eligibility of the natural persons applying for a status, for the purpose of detecting, recognising or identifying natural persons in the context of migration, asylum and border control management, with the exception of verification of travel documents. AI systems in the area of migration, asylum and border control management covered by this Regulation should comply with the relevant procedural requirements set by the Regulation (EC) No 810/2009 of the European Parliament and

用于自然人健康和人寿保险的风险评估和定价的人工智能系统也可能对个人的生计产生重大影响，如果设计、开发和使用不当，可能侵犯其基本权利，并可能对人们的生命和健康造成严重后果，包括金融排斥和歧视。最后，用于评估和分类自然人紧急呼叫的人工智能系统，或用于在紧急第一响应服务(包括警察、消防和医疗援助)的调度中派遣或确定优先顺序的人工智能系统，以及紧急医疗患者分诊系统，也应被归类为高风险，因为它们在对人的生命和健康及其财产极为关键的情况下作出决策。

(59) 鉴于执法机构的角色和责任，执法机构涉及某些人工智能系统使用的行为

其特点是权力失衡程度显著，可能导致监视、逮捕或剥夺自然人的自由，以及对《宪章》所保障的基本权利的其他不利影响。特别是，如果人工智能系统未使用高质量数据进行训练，在其性能、准确性或稳健性方面不符合适当要求，或者在投放市场或以其他方式投入使用之前未经过适当设计和测试，则可能以歧视性或其他不正确或不公正的方式将某些人单独挑出。此外，行使重要的程序性基本权利，如获得有效补救和公正审判的权利以及辩护权和无罪推定，可能会受到阻碍，特别是在此类人工智能系统不够透明、可解释和缺乏记录的情况下。因此，在相关联盟法和国家法律允许使用的情况下，宜将若干拟用于执法领域的人工智能系统归类为高风险，在这些领域中，准确性、可靠性和透明度尤为重要，以避免不利影响、保持公众信任并确保问责和有效补救。鉴于活动的性质及相关风险，这些高风险人工智能系统应特别包括拟由执法当局或代表执法当局使用，或由联盟机构、机关、办事处或机构为支持执法当局而使用的人工智能系统，用于评估自然人成为刑事犯罪受害者的风险(如测谎仪和类似工具)，用于在刑事犯罪调查或起诉过程中评估证据的可靠性，以及在本文例不禁止的情况下，用于评估自然人犯罪或再次犯罪的风险(不仅基于对自然人的特征分析或对自然人或群体的性格特征或过往犯罪行为的评估)，用于在刑事犯罪侦查、调查或起诉过程中进行特征分析。专门拟用于税务和海关当局以及金融情报机构(根据联盟反洗钱法律执行分析信息的行政任务)的行政诉讼的人工智能系统，不应被归类为执法当局为预防、侦查、调查和起诉刑事犯罪而使用的高风险人工智能系统。执法当局和其他相关当局使用人工智能工具不应成为不平等或排斥的因素。不应忽视人工智能工具的使用对嫌疑人辩护权的影响，特别是难以获得关于这些系统运作的有意义信息，以及由此难以在法庭上质疑其结果，特别是对被调查的自然人而言。

(60) 用于移民、庇护和边境管制管理的人工智能系统会影响那些通常处于特别

处于弱势地位并依赖主管公共当局行动结果的人员。因此，在这些情境中使用的人工智能系统的准确性、非歧视性和透明度对于保障受影响人员的基本权利尤为重要，特别是其自由流动、不受歧视、保护私生活和个人数据、国际保护及良好行政的权利。因此，在相关联盟法和国家法律允许其使用的情况下，宜将以下人工智能系统归类为高风险：拟由主管公共当局或代表其使用，或由负责移民、庇护和边境管制管理领域任务的联盟机构、机关、办事处或机构使用的测谎仪及类似工具，用于评估自然人进入成员国领土或申请签证或庇护所构成的某些风险；用于协助主管公共当局审查庇护、签证和居留许可申请及相关申诉，包括对证据可靠性的相关评估，以确定申请身份的自然人的资格；用于在移民、庇护和边境管制管理背景下检测、识别或辨认自然人，但旅行证件验证除外。本 Regulation 所涵盖的移民、庇护和边境管制管理领域的人工智能系统应遵守欧洲议会和理事会 Regulation (EC) No 810/2009 规定的相关程序要求，以及

of the Council ([32]), the Directive 2013/32/EU of the European Parliament and of the Council ([33]), and other relevant Union law. The use of AI systems in migration, asylum and border control management should, in no circumstances, be used by Member States or Union institutions, bodies, offices or agencies as a means to circumvent their international obligations under the UN Convention relating to the Status of Refugees done at Geneva on 28 July 1951 as amended by the Protocol of 31 January 1967. Nor should they be used to in any way infringe on the principle of non-refoulement, or to deny safe and effective legal avenues into the territory of the Union, including the right to international protection.

(61) Certain AI systems intended for the administration of justice and democratic processes should be classified as high-risk, considering their potentially significant impact on democracy, the rule of law, individual freedoms as well as the right to an effective remedy and to a fair trial. In particular, to address the risks of potential biases, errors and opacity, it is appropriate to qualify as high-risk AI systems intended to be used by a judicial authority or on its behalf to assist judicial authorities in researching and interpreting facts and the law and in applying the law to a concrete set of facts. AI systems intended to be used by alternative dispute resolution bodies for those purposes should also be considered to be high-risk when the outcomes of the alternative dispute resolution proceedings produce legal effects for the parties. The use of AI tools can support the decision-making power of judges or judicial independence, but should not replace it: the final decision-making must remain a human-driven activity. The classification of AI systems as high-risk should not, however, extend to AI systems intended for purely ancillary administrative activities that do not affect the actual administration of justice in individual cases, such as anonymisation or pseudonymisation of judicial decisions, documents or data, communication between personnel, administrative tasks.

(62) Without prejudice to the rules provided for in Regulation (EU) 2024/900 of the European Parliament and of the Council ([34]), and in order to address the risks of undue external interference with the right to vote enshrined in Article 39 of the Charter, and of adverse effects on democracy and the rule of law, AI systems intended to be used to influence the outcome of an election or referendum or the voting behaviour of natural persons in the exercise of their vote in elections or referenda should be classified as high-risk AI systems with the exception of AI systems whose output natural persons are not directly exposed to, such as tools used to organise, optimise and structure political campaigns from an administrative and logistical point of view.

(63) The fact that an AI system is classified as a high-risk AI system under this Regulation should not be interpreted as indicating that the use of the system is lawful under other acts of Union law or under national law compatible with Union law, such as on the protection of personal data, on the use of polygraphs and similar tools or other systems to detect the emotional state of natural persons. Any such use should continue to occur solely in accordance with the applicable requirements resulting from the Charter and from the applicable acts of secondary Union law and national law. This Regulation should not be understood as providing for the legal ground for processing of personal data, including special categories of personal data, where relevant, unless it is specifically otherwise provided for in this Regulation.

(64) To mitigate the risks from high-risk AI systems placed on the market or put into service and to ensure a high level of trustworthiness, certain mandatory requirements should apply to high-risk AI systems, taking into account the intended purpose and the context of use of the AI system and according to the risk-management system to be established by the provider. The measures adopted by the providers to comply with the mandatory requirements of this Regulation should take into account the generally acknowledged state of the art on AI, be proportionate and effective to meet the objectives of this Regulation. Based on the New Legislative Framework, as clarified in Commission notice 'The "Blue Guide" on the implementation of EU product rules 2022', the general rule is that more than one legal act of Union harmonisation legislation may be applicable to one product, since the making available or putting into service can take place only when the product complies with all applicable Union harmonisation legislation. The hazards of AI systems covered by the requirements of this Regulation concern different aspects than the existing Union harmonisation legislation and therefore the requirements of this Regulation would complement the existing body of the Union harmonisation legislation. For example, machinery or medical devices products incorporating an AI system might present risks not addressed by the essential health and safety

([32]) Regulation (EC) No 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code) (OJ L 243, 15.9.2009, p. 1).
([33]) Directive 2013/32/EU of the European Parliament and of the Council of 26 June 2013 on common procedures for granting and withdrawing international protection (OJ L 180, 29.6.2013, p. 60).
([34]) Regulation (EU) 2024/900 of the European parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising (OJ L, 2024/900, 20.3.2024, ELI: http://data.europa.eu/eli/reg/2024/900/oj).

理事会第2013/32/EU号指令(32)、欧洲议会和理事会第2013/32/EU号指令(33)以及其他相关联盟法律。成员国或联盟机构、机关、办事处或机构在任何情况下均不得将移民、庇护和边境管制管理中使用人工智能系统作为规避其根据1951年7月28日在日内瓦缔结的《联合国关于难民地位的公约》(经1967年1月31日议定书修正)所承担的国际义务的手段。也不得利用这些系统以任何方式侵犯不驱回原则，或拒绝进入联盟领土的安全有效法律途径，包括获得国际保护的权利。

(61) 某些旨在用于司法行政和民主进程的人工智能系统应被归类为

高风险，考虑到它们对民主、法治、个人自由以及获得有效补救和公正审判的权利的潜在重大影响。特别是，为应对潜在偏见、错误和不透明的风险，宜将拟由司法机关或代表司法机关使用，以协助司法机关研究和解释事实和法律以及将法律适用于具体事实集合的人工智能系统定性为高风险人工智能系统。拟由替代性争议解决机构为此目的使用的人工智能系统，当替代性争议解决程序的结果对当事方产生法律效力时，也应被视为高风险。人工智能工具的使用可以支持法官的决策权或司法独立性，但不应取代之：最终决策必须仍然是人类驱动的活动。然而，将人工智能系统归类为高风险不应扩展到仅用于不影响个案中实际司法行政的纯辅助性行政活动的人工智能系统，如司法判决、文件或数据的匿名化或假名化、人员之间的通信、行政任务。

(62) 在不影响欧洲议会和理事会Regulation (EU) 2024/900所规定规则的情况下

理事会(34)，以及为应对不当外部干预《宪章》第39条所载投票权的风险，以及对民主和法治的不利影响，旨在用于影响选举或公投结果或自然人在选举或公投中行使投票时的投票行为的人工智能系统，应被归类为高风险人工智能系统，但自然人不会直接接触其输出的人工智能系统除外，例如用于从行政和后勤角度组织、优化和构建政治活动的工具。

(63) 人工智能系统根据本条例被归类为高风险人工智能系统这一事实，不应被解释为

表明该系统的使用根据其他欧盟法律或与欧盟法律兼容的国家法律是合法的，例如关于个人数据保护、关于测谎仪和类似工具或其他用于检测自然人情绪状态的系统的法律。任何此类使用应继续仅依照《宪章》以及适用的欧盟二级法律和国家法律所产生的适用要求进行。本法规不应被理解为为个人数据的处理提供法律依据，包括在相关情况下特殊类别的个人数据，除非本法规另有具体规定。

(64) 为减轻投放市场或投入使用的高风险人工智能系统带来的风险，并确保高水平

可信性，某些强制性要求应适用于高风险人工智能系统，同时考虑到人工智能系统的预期目的和使用背景，并根据提供者将建立的风险管理系统。提供者为遵守本法规的强制性要求而采取的措施应考虑到人工智能领域公认的最新水平，应是相称且有效的，以实现本法规的目标。基于新立法框架，正如委员会通知《2022年欧盟产品规则实施"蓝皮书"》所澄清的，一般规则是，多个欧盟协调立法法案可能适用于一个产品，因为只有当产品符合所有适用的欧盟协调立法时，才能进行提供或投入使用。本法规要求所涵盖的人工智能系统的危害涉及与现有欧盟协调立法不同的方面，因此本法规的要求将补充现有的欧盟协调立法体系。例如，包含人工智能系统的机械或医疗器械产品可能存在相关欧盟协调立法中规定的基本健康和安全要求未涉及的风险，

(32) 欧洲议会和理事会2009年7月13日关于制定共同体签证法典(签证法典)的第810/2009号条例(EC)(OJ L 243, 15.9.2009, p.1)。
(33) 欧洲议会和理事会2013年6月26日关于给予和撤销国际保护共同程序的Directive 2013/32/EU(OJ L 180, 29.6.2013, p.60)。
(34) 欧洲议会和理事会2024年3月13日关于政治广告透明度和定向投放的Regulation (EU) 2024/900(OJ L, 2024/900, 20.3.2024, ELI: http://data.europa.eu/eli/reg/2024/900/oj)。

requirements set out in the relevant Union harmonised legislation, as that sectoral law does not deal with risks specific to AI systems. This calls for a simultaneous and complementary application of the various legislative acts. To ensure consistency and to avoid an unnecessary administrative burden and unnecessary costs, providers of a product that contains one or more high-risk AI system, to which the requirements of this Regulation and of the Union harmonisation legislation based on the New Legislative Framework and listed in an annex to this Regulation apply, should have flexibility with regard to operational decisions on how to ensure compliance of a product that contains one or more AI systems with all the applicable requirements of that Union harmonised legislation in an optimal manner. That flexibility could mean, for example a decision by the provider to integrate a part of the necessary testing and reporting processes, information and documentation required under this Regulation into already existing documentation and procedures required under existing Union harmonisation legislation based on the New Legislative Framework and listed in an annex to this Regulation. This should not, in any way, undermine the obligation of the provider to comply with all the applicable requirements.

(65) The risk-management system should consist of a continuous, iterative process that is planned and run throughout the entire lifecycle of a high-risk AI system. That process should be aimed at identifying and mitigating the relevant risks of AI systems on health, safety and fundamental rights. The risk-management system should be regularly reviewed and updated to ensure its continuing effectiveness, as well as justification and documentation of any significant decisions and actions taken subject to this Regulation. This process should ensure that the provider identifies risks or adverse impacts and implements mitigation measures for the known and reasonably foreseeable risks of AI systems to the health, safety and fundamental rights in light of their intended purpose and reasonably foreseeable misuse, including the possible risks arising from the interaction between the AI system and the environment within which it operates. The risk-management system should adopt the most appropriate risk-management measures in light of the state of the art in AI. When identifying the most appropriate risk-management measures, the provider should document and explain the choices made and, when relevant, involve experts and external stakeholders. In identifying the reasonably foreseeable misuse of high-risk AI systems, the provider should cover uses of AI systems which, while not directly covered by the intended purpose and provided for in the instruction for use may nevertheless be reasonably expected to result from readily predictable human behaviour in the context of the specific characteristics and use of a particular AI system. Any known or foreseeable circumstances related to the use of the high-risk AI system in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may lead to risks to the health and safety or fundamental rights should be included in the instructions for use that are provided by the provider. This is to ensure that the deployer is aware and takes them into account when using the high-risk AI system. Identifying and implementing risk mitigation measures for foreseeable misuse under this Regulation should not require specific additional training for the high-risk AI system by the provider to address foreseeable misuse. The providers however are encouraged to consider such additional training measures to mitigate reasonable foreseeable misuses as necessary and appropriate.

(66) Requirements should apply to high-risk AI systems as regards risk management, the quality and relevance of data sets used, technical documentation and record-keeping, transparency and the provision of information to deployers, human oversight, and robustness, accuracy and cybersecurity. Those requirements are necessary to effectively mitigate the risks for health, safety and fundamental rights. As no other less trade restrictive measures are reasonably available those requirements are not unjustified restrictions to trade.

(67) High-quality data and access to high-quality data plays a vital role in providing structure and in ensuring the performance of many AI systems, especially when techniques involving the training of models are used, with a view to ensure that the high-risk AI system performs as intended and safely and it does not become a source of discrimination prohibited by Union law. High-quality data sets for training, validation and testing require the implementation of appropriate data governance and management practices. Data sets for training, validation and testing, including the labels, should be relevant, sufficiently representative, and to the best extent possible free of errors and complete in view of the intended purpose of the system. In order to facilitate compliance with Union data protection law, such as Regulation (EU) 2016/679, data governance and management practices should include, in the case of personal data, transparency about the original purpose of the data collection. The data sets should also have the appropriate statistical properties, including as regards the persons or groups of persons in relation to whom the high-risk AI system is intended to be used, with specific attention to the mitigation of possible biases in the data sets, that are likely to affect the health and safety of persons, have a negative impact on fundamental rights or lead to discrimination prohibited under Union law, especially where data outputs influence inputs for future operations

因为该部门法不处理人工智能系统特有的风险。这要求同时和互补地适用各种立法法案。为确保一致性并避免不必要的行政负担和不必要的成本，对于包含一个或多个高风险人工智能系统且本法规的要求以及基于新立法框架并列入本法规附件中的欧盟协调立法的要求适用于其的产品，其提供者应在如何以最佳方式确保包含一个或多个人工智能系统的产品符合该欧盟协调立法的所有适用要求的操作决策方面具有灵活性。这种灵活性可以意味着，例如，提供者决定将本法规所要求的必要测试和报告流程、信息和文件的一部分整合到基于新立法框架并列入本法规附件的现有欧盟协调立法所要求的现有文件和程序中。这不应以任何方式损害提供者遵守所有适用要求的义务。

(65) 风险管理体系应由一个持续的、迭代的过程组成，该过程在整个

高风险人工智能系统的整个生命周期。该过程应旨在识别和减轻人工智能系统对健康、安全和基本权利的相关风险。风险管理系统应定期审查和更新，以确保其持续有效性，以及对根据本法规作出的任何重大决定和行动的正当性和记录。该过程应确保提供者识别风险或不利影响，并针对人工智能系统对其预期目的和合理可预见的误用(包括人工智能系统与其运行环境之间相互作用可能产生的风险)对健康、安全和基本权利的已知和合理可预见的风险实施缓解措施。风险管理系统应根据人工智能的最新水平采取最适当的风险管理措施。在确定最适当的风险管理措施时，提供者应记录和解释所作的选择，并在相关时让专家和外部利益相关者参与。在识别高风险人工智能系统的合理可预见的误用时，提供者应涵盖人工智能系统的使用，这些使用虽然不直接属于预期目的并在使用说明中规定，但在特定人工智能系统的具体特征和使用的背景下，仍可合理预期源于易于预测的人类行为。与按照预期目的或在合理可预见的误用条件下使用高风险人工智能系统相关的任何已知或可预见的情况，可能导致健康和安全或基本权利的风险，应包含在提供者提供的使用说明中。这是为了确保部署者在使用高风险人工智能系统时知晓并考虑到这些情况。根据本法规识别和实施针对可预见误用的风险缓解措施，不应要求提供者对高风险人工智能系统进行特定的额外培训以应对可预见误用。然而，鼓励提供者在必要和适当的情况下考虑此类额外培训措施，以减轻合理可预见的误用。

(66) 要求应适用于高风险人工智能系统，涉及风险管理、所使用数据的质量和相关性

所使用的数据集、技术文档和记录保存、透明度及向部署者提供信息、人类监督，以及稳健性、准确性和网络安全。这些要求对于有效减轻健康、安全和基本权利方面的风险是必要的。由于没有其他合理可用的限制性更小的贸易措施，这些要求并非不合理的贸易限制。

(67) 高质量数据和获取高质量数据在提供结构以及确保

许多人工智能系统的性能，特别是在使用涉及模型训练的技术时，以确保高风险人工智能系统按预期安全运行，并且不会成为联盟法律所禁止的歧视来源。用于训练、验证和测试的高质量数据集需要实施适当的数据治理和管理实践。用于训练、验证和测试的数据集，包括标签，应当相关、具有足够代表性，并尽可能无错误且完整，符合系统的预期目的。为了促进对联盟数据保护法(如Regulation (EU) 2016/679)的遵守，数据治理和管理实践在涉及个人数据时，应当包括数据收集原始目的的透明度。数据集还应当具有适当的统计特性，包括关于高风险人工智能系统预期使用所涉及的人员或人员群体，特别关注减轻数据集中可能影响人员健康和安全、对基本权利产生负面影响或导致联盟法律所禁止的歧视的可能偏见，尤其是在数据输出影响未来操作的输入时。

(feedback loops). Biases can for example be inherent in underlying data sets, especially when historical data is being used, or generated when the systems are implemented in real world settings. Results provided by AI systems could be influenced by such inherent biases that are inclined to gradually increase and thereby perpetuate and amplify existing discrimination, in particular for persons belonging to certain vulnerable groups, including racial or ethnic groups. The requirement for the data sets to be to the best extent possible complete and free of errors should not affect the use of privacy-preserving techniques in the context of the development and testing of AI systems. In particular, data sets should take into account, to the extent required by their intended purpose, the features, characteristics or elements that are particular to the specific geographical, contextual, behavioural or functional setting which the AI system is intended to be used. The requirements related to data governance can be complied with by having recourse to third parties that offer certified compliance services including verification of data governance, data set integrity, and data training, validation and testing practices, as far as compliance with the data requirements of this Regulation are ensured.

(68) For the development and assessment of high-risk AI systems, certain actors, such as providers, notified bodies and other relevant entities, such as European Digital Innovation Hubs, testing experimentation facilities and researchers, should be able to access and use high-quality data sets within the fields of activities of those actors which are related to this Regulation. European common data spaces established by the Commission and the facilitation of data sharing between businesses and with government in the public interest will be instrumental to provide trustful, accountable and non-discriminatory access to high-quality data for the training, validation and testing of AI systems. For example, in health, the European health data space will facilitate non-discriminatory access to health data and the training of AI algorithms on those data sets, in a privacy-preserving, secure, timely, transparent and trustworthy manner, and with an appropriate institutional governance. Relevant competent authorities, including sectoral ones, providing or supporting the access to data may also support the provision of high-quality data for the training, validation and testing of AI systems.

(69) The right to privacy and to protection of personal data must be guaranteed throughout the entire lifecycle of the AI system. In this regard, the principles of data minimisation and data protection by design and by default, as set out in Union data protection law, are applicable when personal data are processed. Measures taken by providers to ensure compliance with those principles may include not only anonymisation and encryption, but also the use of technology that permits algorithms to be brought to the data and allows training of AI systems without the transmission between parties or copying of the raw or structured data themselves, without prejudice to the requirements on data governance provided for in this Regulation.

(70) In order to protect the right of others from the discrimination that might result from the bias in AI systems, the providers should, exceptionally, to the extent that it is strictly necessary for the purpose of ensuring bias detection and correction in relation to the high-risk AI systems, subject to appropriate safeguards for the fundamental rights and freedoms of natural persons and following the application of all applicable conditions laid down under this Regulation in addition to the conditions laid down in Regulations (EU) 2016/679 and (EU) 2018/1725 and Directive (EU) 2016/680, be able to process also special categories of personal data, as a matter of substantial public interest within the meaning of Article 9(2), point (g) of Regulation (EU) 2016/679 and Article 10(2), point (g) of Regulation (EU) 2018/1725.

(71) Having comprehensible information on how high-risk AI systems have been developed and how they perform throughout their lifetime is essential to enable traceability of those systems, verify compliance with the requirements under this Regulation, as well as monitoring of their operations and post market monitoring. This requires keeping records and the availability of technical documentation, containing information which is necessary to assess the compliance of the AI system with the relevant requirements and facilitate post market monitoring. Such information should include the general characteristics, capabilities and limitations of the system, algorithms, data, training, testing and validation processes used as well as documentation on the relevant risk-management system and drawn in a clear and comprehensive form. The technical documentation should be kept up to date, appropriately throughout the lifetime of the AI system. Furthermore, high-risk AI systems should technically allow for the automatic recording of events, by means of logs, over the duration of the lifetime of the system.

(反馈循环)。偏见例如可能固有于底层数据集中，特别是在使用历史数据时，或者在系统在现实世界环境中实施时产生。人工智能系统提供的结果可能受到此类固有偏见的影响，这些偏见倾向于逐渐增加，从而延续并放大现有的歧视，特别是对于属于某些弱势群体的人员，包括种族或族裔群体。数据集尽可能完整和无错误的要求不应影响在人工智能系统开发和测试背景下使用隐私保护技术。特别是，数据集应当在预期目的所需的范围内，考虑人工智能系统预期使用所针对的特定地理、背景、行为或功能环境的特征、特性或要素。与数据治理相关的要求可以通过求助于提供认证合规服务的第三方来遵守，包括验证数据治理、数据集完整性以及数据训练、验证和测试实践，只要确保遵守本条例的数据要求。

(68) 为开发和评估高风险人工智能系统，某些行为者，如提供者、公告机构和

其他相关实体，如欧洲数字创新中心、测试实验设施和研究人员，应当能够访问和使用与其活动领域相关的、与本条例相关的高质量数据集。委员会建立的欧洲共同数据空间以及促进企业与政府之间为公共利益共享数据，将有助于为人工智能系统的训练、验证和测试提供可信、可问责和非歧视的高质量数据访问。例如，在健康领域，欧洲健康数据空间将促进以隐私保护、安全、及时、透明和可信的方式非歧视地访问健康数据并在这些数据集上训练人工智能算法，并具有适当的机构治理。提供或支持数据访问的相关主管当局，包括部门主管当局，也可以支持为人工智能系统的训练、验证和测试提供高质量数据。

(69) 隐私权和个人数据保护权必须贯穿人工智能的整个生命周期得到保障

系统。在这方面，联盟数据保护法规定的数据最小化和通过设计及默认的数据保护原则适用于个人数据的处理。提供者为确保遵守这些原则而采取的措施不仅应包括匿名化和加密，还应包括使用允许将算法带到数据处并允许训练人工智能系统而无需在各方之间传输或复制原始或结构化数据本身的技术，不影响本条例规定的数据治理要求。

(70) 为保护他人免受人工智能系统中的偏见可能导致的歧视，

提供者应当例外地在严格必要的情况下，为确保与高风险人工智能系统相关的偏见检测和纠正之目的，在针对自然人的基本权利和自由的适当保障措施下，并在适用本条例规定的所有适用条件以及Regulation (EU) 2016/679、Regulation (EU) 2018/1725和Directive (EU) 2016/680规定的条件之后，能够处理特殊类别的个人数据，作为Regulation (EU) 2016/679第9(2)条第(g)点和Regulation (EU) 2018/1725第10(2)条第(g)点含义内的重大公共利益事项。

(71) 拥有关于高风险人工智能系统如何开发及其如何表现的易懂信息

在其整个生命周期内，对于实现这些系统的可追溯性、验证对本条例要求的合规性以及监测其运行和市场后监测至关重要。这要求保存记录并提供技术文档，其中包含评估人工智能系统是否符合相关要求以及促进市场后监测所必需的信息。此类信息应以清晰全面的形式包含系统的一般特征、能力和局限性、所使用的算法、数据、训练、测试和验证过程，以及有关风险管理系统的文档。技术文档应在人工智能系统的整个生命周期内适当保持最新。此外，高风险人工智能系统应在技术上允许在系统整个生命周期内通过日志自动记录事件。

(72) To address concerns related to opacity and complexity of certain AI systems and help deployers to fulfil their obligations under this Regulation, transparency should be required for high-risk AI systems before they are placed on the market or put it into service. High-risk AI systems should be designed in a manner to enable deployers to understand how the AI system works, evaluate its functionality, and comprehend its strengths and limitations. High-risk AI systems should be accompanied by appropriate information in the form of instructions of use. Such information should include the characteristics, capabilities and limitations of performance of the AI system. Those would cover information on possible known and foreseeable circumstances related to the use of the high-risk AI system, including deployer action that may influence system behaviour and performance, under which the AI system can lead to risks to health, safety, and fundamental rights, on the changes that have been pre-determined and assessed for conformity by the provider and on the relevant human oversight measures, including the measures to facilitate the interpretation of the outputs of the AI system by the deployers. Transparency, including the accompanying instructions for use, should assist deployers in the use of the system and support informed decision making by them. Deployers should, inter alia, be in a better position to make the correct choice of the system that they intend to use in light of the obligations applicable to them, be educated about the intended and precluded uses, and use the AI system correctly and as appropriate. In order to enhance legibility and accessibility of the information included in the instructions of use, where appropriate, illustrative examples, for instance on the limitations and on the intended and precluded uses of the AI system, should be included. Providers should ensure that all documentation, including the instructions for use, contains meaningful, comprehensive, accessible and understandable information, taking into account the needs and foreseeable knowledge of the target deployers. Instructions for use should be made available in a language which can be easily understood by target deployers, as determined by the Member State concerned.

(73) High-risk AI systems should be designed and developed in such a way that natural persons can oversee their functioning, ensure that they are used as intended and that their impacts are addressed over the system's lifecycle. To that end, appropriate human oversight measures should be identified by the provider of the system before its placing on the market or putting into service. In particular, where appropriate, such measures should guarantee that the system is subject to in-built operational constraints that cannot be overridden by the system itself and is responsive to the human operator, and that the natural persons to whom human oversight has been assigned have the necessary competence, training and authority to carry out that role. It is also essential, as appropriate, to ensure that high-risk AI systems include mechanisms to guide and inform a natural person to whom human oversight has been assigned to make informed decisions if, when and how to intervene in order to avoid negative consequences or risks, or stop the system if it does not perform as intended. Considering the significant consequences for persons in the case of an incorrect match by certain biometric identification systems, it is appropriate to provide for an enhanced human oversight requirement for those systems so that no action or decision may be taken by the deployer on the basis of the identification resulting from the system unless this has been separately verified and confirmed by at least two natural persons. Those persons could be from one or more entities and include the person operating or using the system. This requirement should not pose unnecessary burden or delays and it could be sufficient that the separate verifications by the different persons are automatically recorded in the logs generated by the system. Given the specificities of the areas of law enforcement, migration, border control and asylum, this requirement should not apply where Union or national law considers the application of that requirement to be disproportionate.

(74) High-risk AI systems should perform consistently throughout their lifecycle and meet an appropriate level of accuracy, robustness and cybersecurity, in light of their intended purpose and in accordance with the generally acknowledged state of the art. The Commission and relevant organisations and stakeholders are encouraged to take due consideration of the mitigation of risks and the negative impacts of the AI system. The expected level of performance metrics should be declared in the accompanying instructions of use. Providers are urged to communicate that information to deployers in a clear and easily understandable way, free of misunderstandings or misleading statements. Union law on legal metrology, including Directives 2014/31/EU ([35]) and 2014/32/EU ([36]) of the European Parliament and of the Council, aims to ensure the accuracy of measurements and to help the transparency and fairness of commercial transactions. In that context, in cooperation with relevant stakeholders and organisation, such as metrology and benchmarking authorities, the Commission should encourage, as appropriate, the development of benchmarks and measurement methodologies for AI systems. In doing so, the Commission should take note and collaborate with international partners working on metrology and relevant measurement indicators relating to AI.

([35]) Directive 2014/31/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of non-automatic weighing instruments (OJ L 96, 29.3.2014, p. 107).

([36]) Directive 2014/32/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of measuring instruments (OJ L 96, 29.3.2014, p. 149).

(72) 为解决与某些人工智能系统的不透明性和复杂性相关的关切，并帮助部署者履行本条例规定的义务，高风险人工智能系统在投放市场或投入使用前应满足透明度要求。高风险人工智能系统的设计应使部署者能够理解人工智能系统的工作原理、评估其功能并了解其优势和局限性。高风险人工智能系统应附有以使用说明形式提供的适当信息。此类信息应包括人工智能系统的特征、能力和性能局限性。这些信息将涵盖与使用高风险人工智能系统相关的可能的已知和可预见情况，包括可能影响系统行为和性能的部署者行为，在这些情况下人工智能系统可能对健康、安全和基本权利造成风险，还应涵盖提供者已预先确定并评估合格性的变更以及相关的人类监督措施，包括便于部署者解释人工智能系统输出的措施。透明度，包括随附的使用说明，应协助部署者使用系统并支持其作出知情决策。部署者尤其应能够根据适用于其的义务更好地正确选择其打算使用的系统，了解预期用途和禁止用途，并正确、适当地使用人工智能系统。为增强使用说明中所含信息的可读性和可获取性，在适当情况下应包含示例性说明，例如关于人工智能系统的局限性和预期及禁止用途的说明。提供者应确保所有文档(包括使用说明)包含有意义、全面、可获取且可理解的信息，同时考虑目标部署者的需求和可预见的知识水平。使用说明应以目标部署者易于理解的语言提供，具体由相关成员国确定。

(73) 高风险人工智能系统的设计和开发应使自然人能够监督其

运行，确保其按预期使用，并在系统生命周期内处理其影响。为此，系统的提供者应在投放市场或投入使用前确定适当的人类监督措施。特别是，在适当情况下，此类措施应保证系统受到系统本身无法覆盖的内置操作约束，并对人类操作者作出响应，且被指派人类监督的自然人具备履行该职责所需的能力、培训和权限。在适当情况下，还应确保高风险人工智能系统包含相关机制，指导和告知被指派人类监督的自然人在何时以及如何干预以作出知情决策，以避免负面后果或风险，或在系统未按预期运行时停止系统。考虑到某些生物识别系统在错误匹配时对个人造成的重大后果，宜对此类系统规定强化的人类监督要求，以便部署者不得基于系统产生的识别结果采取任何行动或作出任何决定，除非该结果已由至少两名自然人单独核实和确认。这些人员可来自一个或多个实体，并包括操作或使用系统的人员。该要求不应造成不必要的负担或延迟，不同人员分别进行的核实自动记录在系统生成的日志中即可满足要求。鉴于执法、移民、边境控制和庇护领域的特殊性，在联盟法或国家法律认为适用该要求不适当的情况下，该要求不应适用。

(74) 高风险人工智能系统应在其整个生命周期内保持一致的性能，并达到适当水平的

准确性、稳健性和网络安全，同时考虑其预期用途并依照公认的最新水平。鼓励委员会及相关组织和利益相关者适当考虑减轻人工智能系统的风险和负面影响。预期的性能指标水平应在随附的使用说明中声明。敦促提供者以清晰易懂的方式向部署者传达该信息，避免误解或误导性陈述。关于法定计量的联盟法，包括欧洲议会和理事会第2014/31/EU号指令(35)和第2014/32/EU号指令(36)，旨在确保测量的准确性并促进商业交易的透明度和公平性。在此背景下，委员会应与相关利益相关者和组织(如计量和基准测试机构)合作，酌情鼓励制定人工智能系统的基准和测量方法。在此过程中，委员会应注意并与从事计量和人工智能相关测量指标工作的国际伙伴合作。

(35) 欧洲议会和理事会2014年2月26日关于协调成员国有关非自动衡器投放市场的法律的指令2014/31/EU(OJ L 96, 29.3.2014, p.107)。

(36) 欧洲议会和理事会2014年2月26日关于协调成员国有关测量仪器投放市场法律的指令2014/32/EU(OJ L 96, 29.3.2014, p.149)。

(75) Technical robustness is a key requirement for high-risk AI systems. They should be resilient in relation to harmful or otherwise undesirable behaviour that may result from limitations within the systems or the environment in which the systems operate (e.g. errors, faults, inconsistencies, unexpected situations). Therefore, technical and organisational measures should be taken to ensure robustness of high-risk AI systems, for example by designing and developing appropriate technical solutions to prevent or minimise harmful or otherwise undesirable behaviour. Those technical solution may include for instance mechanisms enabling the system to safely interrupt its operation (fail-safe plans) in the presence of certain anomalies or when operation takes place outside certain predetermined boundaries. Failure to protect against these risks could lead to safety impacts or negatively affect the fundamental rights, for example due to erroneous decisions or wrong or biased outputs generated by the AI system.

(76) Cybersecurity plays a crucial role in ensuring that AI systems are resilient against attempts to alter their use, behaviour, performance or compromise their security properties by malicious third parties exploiting the system's vulnerabilities. Cyberattacks against AI systems can leverage AI specific assets, such as training data sets (e.g. data poisoning) or trained models (e.g. adversarial attacks or membership inference), or exploit vulnerabilities in the AI system's digital assets or the underlying ICT infrastructure. To ensure a level of cybersecurity appropriate to the risks, suitable measures, such as security controls, should therefore be taken by the providers of high-risk AI systems, also taking into account as appropriate the underlying ICT infrastructure.

(77) Without prejudice to the requirements related to robustness and accuracy set out in this Regulation, high-risk AI systems which fall within the scope of a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements, in accordance with that regulation may demonstrate compliance with the cybersecurity requirements of this Regulation by fulfilling the essential cybersecurity requirements set out in that regulation. When high-risk AI systems fulfil the essential requirements of a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements, they should be deemed compliant with the cybersecurity requirements set out in this Regulation in so far as the achievement of those requirements is demonstrated in the EU declaration of conformity or parts thereof issued under that regulation. To that end, the assessment of the cybersecurity risks, associated to a product with digital elements classified as high-risk AI system according to this Regulation, carried out under a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements, should consider risks to the cyber resilience of an AI system as regards attempts by unauthorised third parties to alter its use, behaviour or performance, including AI specific vulnerabilities such as data poisoning or adversarial attacks, as well as, as relevant, risks to fundamental rights as required by this Regulation.

(78) The conformity assessment procedure provided by this Regulation should apply in relation to the essential cybersecurity requirements of a product with digital elements covered by a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and classified as a high-risk AI system under this Regulation. However, this rule should not result in reducing the necessary level of assurance for critical products with digital elements covered by a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements. Therefore, by way of derogation from this rule, high-risk AI systems that fall within the scope of this Regulation and are also qualified as important and critical products with digital elements pursuant to a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and to which the conformity assessment procedure based on internal control set out in an annex to this Regulation applies, are subject to the conformity assessment provisions of a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements insofar as the essential cybersecurity requirements of that regulation are concerned. In this case, for all the other aspects covered by this Regulation the respective provisions on conformity assessment based on internal control set out in an annex to this Regulation should apply. Building on the knowledge and expertise of ENISA on the cybersecurity policy and tasks assigned to ENISA under the Regulation (EU) 2019/881 of the European Parliament and of the Council ([37]), the Commission should cooperate with ENISA on issues related to cybersecurity of AI systems.

([37]) Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15).

(75) 技术稳健性是高风险人工智能系统的一项关键要求。它们应能够抵御可能因系统内部或系统运行环境的局限性而产生的有害或其他不良行为(例如错误、故障、不一致、意外情况)。因此，应采取技术和组织措施确保高风险人工智能系统的稳健性，例如通过设计和开发适当的技术解决方案来防止或尽量减少有害或其他不良行为。这些技术解决方案可包括使系统能够在出现某些异常或在一定预定边界之外运行时安全中断其运行的机制(故障安全计划)。未能防范这些风险可能导致安全影响或对基本权利产生负面影响，例如由于人工智能系统产生的错误决策或错误或有偏见的输出。

(76) 网络安全在确保人工智能系统能够抵御改变其用途的企图方面发挥着关键作用，

行为、性能或损害其安全属性，由恶意第三方利用系统脆弱性实施。针对人工智能系统的网络攻击可能利用人工智能特有的资产，例如训练数据集(例如数据投毒)或已训练的模型(例如对抗性攻击或成员推断)，或利用人工智能系统数字资产或底层信息通信技术基础设施中的脆弱性。因此，为确保与风险相适应的网络安全水平，高风险人工智能系统的提供者应采取适当措施，例如安全控制，并酌情考虑底层信息通信技术基础设施。

(77) 在不影响本条例规定的稳健性和准确性相关要求的情况下，高风险人工智能

属于欧洲议会和理事会关于含数字元素产品横向网络安全要求的条例范围内的系统，可根据该条例通过满足该条例规定的基本网络安全要求来证明符合本条例的网络安全要求。当高风险人工智能系统满足欧洲议会和理事会关于含数字元素产品横向网络安全要求的条例的基本要求时，在根据该条例签发的欧盟符合性声明或其部分中证明实现了这些要求的范围内，应视为符合本条例规定的网络安全要求。为此，根据欧洲议会和理事会关于含数字元素产品横向网络安全要求的条例，对根据本条例被归类为高风险人工智能系统的含数字元素产品所进行的网络安全风险评估，应考虑人工智能系统在网络韧性方面面临未经授权的第三方试图改变其使用、行为或性能的风险，包括数据投毒或对抗性攻击等人工智能特有的脆弱性，以及酌情考虑本条例所要求的基本权利风险。

(78) 本法规规定的合格评定程序应适用于基本

受欧洲议会和理事会关于含数字元素产品横向网络安全要求的条例涵盖并根据本条例被归类为高风险人工智能系统的含数字元素产品的网络安全要求。然而，该规则不应导致降低受欧洲议会和理事会关于含数字元素产品横向网络安全要求的条例涵盖的关键含数字元素产品所必需的保证水平。因此，作为对该规则的减损，属于本条例范围且根据欧洲议会和理事会关于含数字元素产品横向网络安全要求的条例同时被认定为重要和关键含数字元素产品、且适用本条例附件中规定的基于内部控制的合格评定程序的高风险人工智能系统，在涉及该条例的基本网络安全要求方面，适用欧洲议会和理事会关于含数字元素产品横向网络安全要求的条例的合格评定规定。在此情况下，对于本条例涵盖的所有其他方面，应适用本条例附件中规定的基于内部控制的合格评定相应规定。基于ENISA在网络安全政策方面的知识和专长以及根据欧洲议会和理事会条例(EU) 2019/881(37)赋予ENISA的任务，委员会应与ENISA就人工智能系统网络安全相关问题开展合作。

(37) 欧洲议会和理事会2019年4月17日关于ENISA(欧盟网络安全局)及信息与通信技术网络安全认证并废止第526/2013号条例(欧盟)的第2019/881号条例(欧盟)(《网络安全法案》)(OJ L 151, 7.6.2019, p.15)。

(79) It is appropriate that a specific natural or legal person, defined as the provider, takes responsibility for the placing on the market or the putting into service of a high-risk AI system, regardless of whether that natural or legal person is the person who designed or developed the system.

(80) As signatories to the United Nations Convention on the Rights of Persons with Disabilities, the Union and the Member States are legally obliged to protect persons with disabilities from discrimination and promote their equality, to ensure that persons with disabilities have access, on an equal basis with others, to information and communications technologies and systems, and to ensure respect for privacy for persons with disabilities. Given the growing importance and use of AI systems, the application of universal design principles to all new technologies and services should ensure full and equal access for everyone potentially affected by or using AI technologies, including persons with disabilities, in a way that takes full account of their inherent dignity and diversity. It is therefore essential that providers ensure full compliance with accessibility requirements, including Directive (EU) 2016/2102 of the European Parliament and of the Council ([38]) and Directive (EU) 2019/882. Providers should ensure compliance with these requirements by design. Therefore, the necessary measures should be integrated as much as possible into the design of the high-risk AI system.

(81) The provider should establish a sound quality management system, ensure the accomplishment of the required conformity assessment procedure, draw up the relevant documentation and establish a robust post-market monitoring system. Providers of high-risk AI systems that are subject to obligations regarding quality management systems under relevant sectoral Union law should have the possibility to include the elements of the quality management system provided for in this Regulation as part of the existing quality management system provided for in that other sectoral Union law. The complementarity between this Regulation and existing sectoral Union law should also be taken into account in future standardisation activities or guidance adopted by the Commission. Public authorities which put into service high-risk AI systems for their own use may adopt and implement the rules for the quality management system as part of the quality management system adopted at a national or regional level, as appropriate, taking into account the specificities of the sector and the competences and organisation of the public authority concerned.

(82) To enable enforcement of this Regulation and create a level playing field for operators, and, taking into account the different forms of making available of digital products, it is important to ensure that, under all circumstances, a person established in the Union can provide authorities with all the necessary information on the compliance of an AI system. Therefore, prior to making their AI systems available in the Union, providers established in third countries should, by written mandate, appoint an authorised representative established in the Union. This authorised representative plays a pivotal role in ensuring the compliance of the high-risk AI systems placed on the market or put into service in the Union by those providers who are not established in the Union and in serving as their contact person established in the Union.

(83) In light of the nature and complexity of the value chain for AI systems and in line with the New Legislative Framework, it is essential to ensure legal certainty and facilitate the compliance with this Regulation. Therefore, it is necessary to clarify the role and the specific obligations of relevant operators along that value chain, such as importers and distributors who may contribute to the development of AI systems. In certain situations those operators could act in more than one role at the same time and should therefore fulfil cumulatively all relevant obligations associated with those roles. For example, an operator could act as a distributor and an importer at the same time.

(84) To ensure legal certainty, it is necessary to clarify that, under certain specific conditions, any distributor, importer, deployer or other third-party should be considered to be a provider of a high-risk AI system and therefore assume all the relevant obligations. This would be the case if that party puts its name or trademark on a high-risk AI system already placed on the market or put into service, without prejudice to contractual arrangements stipulating that the obligations are allocated otherwise. This would also be the case if that party makes a substantial modification to a high-risk AI system that has already been placed on the market or has already been put into service in a way that it remains a high-risk AI system in accordance with this Regulation, or if it modifies the intended purpose of an AI system, including a general-purpose AI system, which has not been classified as high-risk and has already been placed on the market or put into service, in a way that the AI system becomes a high-risk AI system in accordance with this Regulation. Those provisions should apply without prejudice to more specific provisions established in certain Union harmonisation legislation based on the New Legislative Framework, together with which this

([38]) Directive (EU) 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the accessibility of the websites and mobile applications of public sector bodies (OJ L 327, 2.12.2016, p. 1).

(79) 宜由被定义为提供者的特定自然人或法人对高风险人工智能系统的投放市场或投入使用承担责任，无论该自然人或法人是否为设计或开发该系统的人。

(80) 作为《联合国残疾人权利公约》的签署方，欧盟和成员国有法律义务保护残疾人免受歧视并促进其平等，确保残疾人在与其他人平等的基础上获得信息和通信技术及系统，并确保尊重残疾人的隐私。鉴于人工智能系统的重要性和使用日益增加，将通用设计原则应用于所有新技术和服务应确保所有可能受人工智能技术影响或使用人工智能技术的人，包括残疾人，能够充分和平等地获取，并充分考虑到其固有尊严和多样性。因此，提供者必须确保完全遵守无障碍要求，包括欧洲议会和理事会指令(EU) 2016/2102(38)和指令(EU) 2019/882。提供者应通过设计确保遵守这些要求。因此，必要措施应尽可能纳入高风险人工智能系统的设计中。

(81) 提供者应建立完善的质量管理体系，确保完成所需的合格评定程序，编制相关文件并建立稳健的上市后监测系统。受相关行业联盟法律下质量管理体系义务约束的高风险人工智能系统的提供者，应有可能将本条例规定的质量管理体系要素作为该其他行业联盟法律规定的现有质量管理体系的一部分纳入。本条例与现有行业联盟法律之间的互补性也应在委员会未来通过的标准化活动或指南中予以考虑。为自身使用而将高风险人工智能系统投入使用的公共机构，可酌情在国家或地区层面采用的质量管理体系中采纳和实施质量管理体系规则，同时考虑相关行业的特点以及公共机构的权限和组织结构。

(82) 为使本条例得以执行并为运营者创造公平的竞争环境，并考虑到不同形式的数字产品提供方式，必须确保在任何情况下，设立在欧盟境内的个人能够向主管机关提供关于人工智能系统合规性的所有必要信息。因此，设立在第三国的提供者在将其人工智能系统投放欧盟市场之前，应通过书面授权，指定一名设立在欧盟境内的授权代表。该授权代表在确保由未设立在欧盟境内的提供者投放市场或投入服务的高风险人工智能系统的合规性方面，以及作为其设立在欧盟境内的联系人方面，发挥着关键作用。

(83) 鉴于人工智能系统价值链的性质和复杂性，并依照新立法框架，确保法律确定性并促进对本条例的遵守至关重要。因此，有必要明确该价值链上相关运营者的角色和具体义务，例如可能参与人工智能系统开发的进口商和分销商。在某些情况下，这些运营者可能同时担任多个角色，因此应累积履行与这些角色相关的所有相关义务。例如，一个运营者可能同时作为分销商和进口商行事。

(84) 为确保法律确定性，有必要澄清，在某些特定条件下，任何分销商、进口商、部署者或其他第三方应被视为高风险人工智能系统的提供者，并因此承担所有相关义务。如果该方将名称或商标加贴于已投放市场或投入服务的高风险人工智能系统上，即属此种情形，但不影响规定义务另行分配的合同安排。如果该方对已投放市场或已投入服务的高风险人工智能系统进行实质性修改，使其根据本条例仍为高风险人工智能系统，或者如果该方修改尚未被归类为高风险且已投放市场或投入服务的人工智能系统(包括通用人工智能系统)的预期用途，使该人工智能系统根据本条例成为高风险人工智能系统，亦属此种情形。这些规定应不影响基于新立法框架的某些欧盟协调立法中确立的更具体规定，本条例与该等立法

(38) 欧洲议会和理事会2016年10月26日关于公共部门机构网站和移动应用程序无障碍性的指令(EU) 2016/2102(OJ L 327, 2.12.2016， 第1页)。

Regulation should apply. For example, Article 16(2) of Regulation (EU) 2017/745, establishing that certain changes should not be considered to be modifications of a device that could affect its compliance with the applicable requirements, should continue to apply to high-risk AI systems that are medical devices within the meaning of that Regulation.

(85) General-purpose AI systems may be used as high-risk AI systems by themselves or be components of other high-risk AI systems. Therefore, due to their particular nature and in order to ensure a fair sharing of responsibilities along the AI value chain, the providers of such systems should, irrespective of whether they may be used as high-risk AI systems as such by other providers or as components of high-risk AI systems and unless provided otherwise under this Regulation, closely cooperate with the providers of the relevant high-risk AI systems to enable their compliance with the relevant obligations under this Regulation and with the competent authorities established under this Regulation.

(86) Where, under the conditions laid down in this Regulation, the provider that initially placed the AI system on the market or put it into service should no longer be considered to be the provider for the purposes of this Regulation, and when that provider has not expressly excluded the change of the AI system into a high-risk AI system, the former provider should nonetheless closely cooperate and make available the necessary information and provide the reasonably expected technical access and other assistance that are required for the fulfilment of the obligations set out in this Regulation, in particular regarding the compliance with the conformity assessment of high-risk AI systems.

(87) In addition, where a high-risk AI system that is a safety component of a product which falls within the scope of Union harmonisation legislation based on the New Legislative Framework is not placed on the market or put into service independently from the product, the product manufacturer defined in that legislation should comply with the obligations of the provider established in this Regulation and should, in particular, ensure that the AI system embedded in the final product complies with the requirements of this Regulation.

(88) Along the AI value chain multiple parties often supply AI systems, tools and services but also components or processes that are incorporated by the provider into the AI system with various objectives, including the model training, model retraining, model testing and evaluation, integration into software, or other aspects of model development. Those parties have an important role to play in the value chain towards the provider of the high-risk AI system into which their AI systems, tools, services, components or processes are integrated, and should provide by written agreement this provider with the necessary information, capabilities, technical access and other assistance based on the generally acknowledged state of the art, in order to enable the provider to fully comply with the obligations set out in this Regulation, without compromising their own intellectual property rights or trade secrets.

(89) Third parties making accessible to the public tools, services, processes, or AI components other than general-purpose AI models, should not be mandated to comply with requirements targeting the responsibilities along the AI value chain, in particular towards the provider that has used or integrated them, when those tools, services, processes, or AI components are made accessible under a free and open-source licence. Developers of free and open-source tools, services, processes, or AI components other than general-purpose AI models should be encouraged to implement widely adopted documentation practices, such as model cards and data sheets, as a way to accelerate information sharing along the AI value chain, allowing the promotion of trustworthy AI systems in the Union.

(90) The Commission could develop and recommend voluntary model contractual terms between providers of high-risk AI systems and third parties that supply tools, services, components or processes that are used or integrated in high-risk AI systems, to facilitate the cooperation along the value chain. When developing voluntary model contractual terms, the Commission should also take into account possible contractual requirements applicable in specific sectors or business cases.

(91) Given the nature of AI systems and the risks to safety and fundamental rights possibly associated with their use, including as regards the need to ensure proper monitoring of the performance of an AI system in a real-life setting, it is appropriate to set specific responsibilities for deployers. Deployers should in particular take appropriate technical and organisational measures to ensure they use high-risk AI systems in accordance with the instructions of use and certain other obligations should be provided for with regard to monitoring of the functioning of the AI systems and with regard to record-keeping, as appropriate. Furthermore, deployers should ensure that the persons assigned to implement the instructions for use and human oversight as set out in this Regulation have the necessary

本条例应当适用。例如，确立某些变更不应被视为可能影响设备符合适用要求的修改的条例(EU) 2017/745第16(2)条，应当继续适用于属于该条例含义范围内医疗器械的高风险人工智能系统。

(85) 通用人工智能系统可自身作为高风险人工智能系统使用，或作为其他高风险

人工智能系统。因此，鉴于其特殊性质，并为了确保人工智能价值链上责任的公平分担，此类系统的提供者应--无论其是否可能被其他提供者作为高风险人工智能系统本身使用，还是作为高风险人工智能系统的组件使用，且除非本条例另有规定--与相关高风险人工智能系统的提供者密切合作，使其能够遵守本条例下的相关义务以及根据本条例设立的主管机关的要求。

(86) 在符合本法规规定的条件下，最初将人工智能系统投放

市场或投入服务，则不应再被视为本条例意义上的提供者；且当该提供者未明确排除将人工智能系统变更为高风险人工智能系统时，原提供者仍应密切合作，提供必要信息，并提供履行本条例规定义务所需的合理预期的技术访问和其他协助，特别是在高风险人工智能系统合格评定合规方面。

(87) 此外，如果属于产品安全组件的高风险人工智能系统属于

基于新立法框架的欧盟协调立法，未独立于产品投放市场或投入使用的，该立法中定义的产品制造商应当遵守本条例规定的提供者义务，并尤其应确保嵌入最终产品的人工智能系统符合本条例的要求。

(88) 在人工智能价值链上，多方通常提供人工智能系统、工具和服务，但也提供组件或

提供者出于各种目的纳入人工智能系统的过程，包括模型训练、模型再训练、模型测试与评估、集成到软件中或模型开发的其他方面。这些参与方在价值链中相对于高风险人工智能系统的提供者发挥着重要作用，其人工智能系统、工具、服务、组件或过程被集成到该提供者处，并应通过书面协议向该提供者提供基于公认最新技术水平的必要信息、能力、技术访问和其他协助，以使提供者能够完全遵守本条例规定的义务，同时不损害其自身的知识产权或商业秘密。

(89) 向公众提供工具、服务、流程或人工智能组件（而非

通用人工智能模型，当这些工具、服务、过程或人工智能组件以自由和开源许可证提供时，不应被强制要求遵守针对人工智能价值链上责任的各项要求，特别是对已使用或集成它们之提供者的责任。应鼓励通用人工智能模型以外的自由和开源工具、服务、过程或人工智能组件的开发者实施广泛采用的文档实践，如模型卡和数据表，以加速人工智能价值链上的信息共享，从而促进联盟内可信人工智能系统的推广。

(90) 委员会可制定并推荐高风险人工智能系统提供者与提供用于或集成于高风险人工智能系统的工具、服务、组件或流程的第三方之间的自愿示范合同条款，以促进价值链上的合作。在制定自愿示范合同条款时，委员会还应考虑特定行业或业务情形中可能适用的合同要求。

(91) 鉴于人工智能系统的性质以及其使用可能带来的安全和基本权利风险，

包括在确保对人工智能系统在真实环境中的性能进行适当监测的必要性方面，宜为部署者设定具体责任。部署者尤其应采取适当的技术和组织措施，确保其按照使用说明使用高风险人工智能系统，并应就人工智能系统运行的监测以及酌情就记录保存规定某些其他义务。此外，部署者应确保被指派执行本条例规定的使用说明和人类监督的人员具备必要的

competence, in particular an adequate level of AI literacy, training and authority to properly fulfil those tasks. Those obligations should be without prejudice to other deployer obligations in relation to high-risk AI systems under Union or national law.

(92) This Regulation is without prejudice to obligations for employers to inform or to inform and consult workers or their representatives under Union or national law and practice, including Directive 2002/14/EC of the European Parliament and of the Council ([39]), on decisions to put into service or use AI systems. It remains necessary to ensure information of workers and their representatives on the planned deployment of high-risk AI systems at the workplace where the conditions for those information or information and consultation obligations in other legal instruments are not fulfilled. Moreover, such information right is ancillary and necessary to the objective of protecting fundamental rights that underlies this Regulation. Therefore, an information requirement to that effect should be laid down in this Regulation, without affecting any existing rights of workers.

(93) Whilst risks related to AI systems can result from the way such systems are designed, risks can as well stem from how such AI systems are used. Deployers of high-risk AI system therefore play a critical role in ensuring that fundamental rights are protected, complementing the obligations of the provider when developing the AI system. Deployers are best placed to understand how the high-risk AI system will be used concretely and can therefore identify potential significant risks that were not foreseen in the development phase, due to a more precise knowledge of the context of use, the persons or groups of persons likely to be affected, including vulnerable groups. Deployers of high-risk AI systems listed in an annex to this Regulation also play a critical role in informing natural persons and should, when they make decisions or assist in making decisions related to natural persons, where applicable, inform the natural persons that they are subject to the use of the high-risk AI system. This information should include the intended purpose and the type of decisions it makes. The deployer should also inform the natural persons about their right to an explanation provided under this Regulation. With regard to high-risk AI systems used for law enforcement purposes, that obligation should be implemented in accordance with Article 13 of Directive (EU) 2016/680.

(94) Any processing of biometric data involved in the use of AI systems for biometric identification for the purpose of law enforcement needs to comply with Article 10 of Directive (EU) 2016/680, that allows such processing only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and where authorised by Union or Member State law. Such use, when authorised, also needs to respect the principles laid down in Article 4 (1) of Directive (EU) 2016/680 including lawfulness, fairness and transparency, purpose limitation, accuracy and storage limitation.

(95) Without prejudice to applicable Union law, in particular Regulation (EU) 2016/679 and Directive (EU) 2016/680, considering the intrusive nature of post-remote biometric identification systems, the use of post-remote biometric identification systems should be subject to safeguards. Post-remote biometric identification systems should always be used in a way that is proportionate, legitimate and strictly necessary, and thus targeted, in terms of the individuals to be identified, the location, temporal scope and based on a closed data set of legally acquired video footage. In any case, post-remote biometric identification systems should not be used in the framework of law enforcement to lead to indiscriminate surveillance. The conditions for post-remote biometric identification should in any case not provide a basis to circumvent the conditions of the prohibition and strict exceptions for real time remote biometric identification.

(96) In order to efficiently ensure that fundamental rights are protected, deployers of high-risk AI systems that are bodies governed by public law, or private entities providing public services and deployers of certain high-risk AI systems listed in an annex to this Regulation, such as banking or insurance entities, should carry out a fundamental rights impact assessment prior to putting it into use. Services important for individuals that are of public nature may also be provided by private entities. Private entities providing such public services are linked to tasks in the public interest such as in the areas of education, healthcare, social services, housing, administration of justice. The aim of the fundamental rights impact assessment is for the deployer to identify the specific risks to the rights of individuals or groups of individuals likely to be affected, identify measures to be taken in the case of a materialisation of those risks. The impact assessment should be performed prior to deploying the high-risk AI system, and should be updated

([39]) Directive 2002/14/EC of the European Parliament and of the Council of 11 March 2002 establishing a general framework for informing and consulting employees in the European Community (OJ L 80, 23.3.2002, p. 29).

能力，特别是适当水平的人工智能素养、培训和权限，以妥善履行这些任务。这些义务不应影响部署者根据欧盟或国家法律在高风险人工智能系统方面的其他义务。

(92) 本法规不影响雇主告知或告知并咨询工人或

其根据联盟或国家法律和实践的代表，包括欧洲议会和理事会第2002/14/EC号指令(39)，就投入服务或使用人工智能系统的决定。在劳动场所其他法律文书中信息或信息与协商义务的条件未得到满足的情况下，仍有必要确保工人及其代表获得关于计划部署高风险人工智能系统的信息。此外，此种信息权是本条例所依据的保护基本权利目标的附属和必要内容。因此，宜在本条例中规定这方面的信息要求，而不影响工人的任何现有权利。

(93) 虽然与人工智能系统相关的风险可能源于此类系统的设计方式，但风险也可能源于此类人工智能系统的使用方式。因此，高风险人工智能系统的部署者在确保基本权利得到保护方面发挥着关键作用，补充提供者在开发人工智能系统时的义务。部署者最适合理解高风险人工智能系统将如何具体使用，因此能够识别在开发阶段未曾预见的潜在重大风险，因为其更准确地了解使用背景、可能受影响的自然人或群体，包括弱势群体。本条例附件所列高风险人工智能系统的部署者在告知自然人方面也发挥着关键作用，并且当其在适用情况下作出或协助作出与自然人相关的决定时，应告知自然人其受到高风险人工智能系统使用的影响。该信息应包括预期目的及其所作决定的类型。部署者还应告知自然人其根据本条例获得解释的权利。对于用于执法目的的高风险人工智能系统，该义务应按照第(EU) 2016/680号指令第13条实施。

(94) 为执法目的使用人工智能系统进行生物特征识别所涉及的任何生物特征数据处理，均需遵守(EU) 2016/680指令第10条，该条仅允许在严格必要、对数据主体权利和自由有适当保障措施、且经联盟或成员国法律授权的情况下进行此类处理。此类使用在获得授权时，还需遵守(EU) 2016/680指令第4(1)条规定的原则，包括合法性、公平性和透明性、目的限制、准确性和存储限制。

(95) 在不影响适用的联盟法律，特别是（欧盟）2016/679号条例和（欧盟）2016/680号指令的前提下，考虑到远程生物特征识别后系统的侵入性，远程生物特征识别后系统的使用应受到保障措施的约束。远程生物特征识别后系统应始终以相称、合法和严格必要的方式使用，因此在被识别个人、地点、时间范围方面应具有针对性，并基于合法获取的视频素材的封闭数据集。在任何情况下，远程生物特征识别后系统不应在执法框架内被用于导致无差别监视。远程生物特征识别后的条件在任何情况下都不应成为规避实时远程生物特征识别禁令和严格例外条件的依据。

(96) 为有效确保基本权利得到保护，属于公法管辖机构的提供者，或提供公共服务的私营实体，以及本法规附件所列某些高风险人工智能系统的部署者，如银行或保险实体，应在投入使用前进行基本权利影响评估。对个人具有重要性的公共服务性质的服务也可由私营实体提供。提供此类公共服务的私营实体与公共利益任务相关联，例如在教育、医疗保健、社会服务、住房、司法行政等领域。基本权利影响评估的目的是让部署者识别可能受影响个人或群体权利的具体风险，确定在这些风险实际发生时应采取的措施。影响评估应在部署高风险人工智能系统之前进行，并应在部署者认为任何相关因素发生变化时予以更新。

(39) 欧洲议会和理事会2002年3月11日关于建立欧洲共同体员工告知和咨询总体框架的指令2002/14/EC(OJ L 80, 23.3.2002， 第29页)。

when the deployer considers that any of the relevant factors have changed. The impact assessment should identify the deployer's relevant processes in which the high-risk AI system will be used in line with its intended purpose, and should include a description of the period of time and frequency in which the system is intended to be used as well as of specific categories of natural persons and groups who are likely to be affected in the specific context of use. The assessment should also include the identification of specific risks of harm likely to have an impact on the fundamental rights of those persons or groups. While performing this assessment, the deployer should take into account information relevant to a proper assessment of the impact, including but not limited to the information given by the provider of the high-risk AI system in the instructions for use. In light of the risks identified, deployers should determine measures to be taken in the case of a materialisation of those risks, including for example governance arrangements in that specific context of use, such as arrangements for human oversight according to the instructions of use or, complaint handling and redress procedures, as they could be instrumental in mitigating risks to fundamental rights in concrete use-cases. After performing that impact assessment, the deployer should notify the relevant market surveillance authority. Where appropriate, to collect relevant information necessary to perform the impact assessment, deployers of high-risk AI system, in particular when AI systems are used in the public sector, could involve relevant stakeholders, including the representatives of groups of persons likely to be affected by the AI system, independent experts, and civil society organisations in conducting such impact assessments and designing measures to be taken in the case of materialisation of the risks. The European Artificial Intelligence Office (AI Office) should develop a template for a questionnaire in order to facilitate compliance and reduce the administrative burden for deployers.

(97) The notion of general-purpose AI models should be clearly defined and set apart from the notion of AI systems to enable legal certainty. The definition should be based on the key functional characteristics of a general-purpose AI model, in particular the generality and the capability to competently perform a wide range of distinct tasks. These models are typically trained on large amounts of data, through various methods, such as self-supervised, unsupervised or reinforcement learning. General-purpose AI models may be placed on the market in various ways, including through libraries, application programming interfaces (APIs), as direct download, or as physical copy. These models may be further modified or fine-tuned into new models. Although AI models are essential components of AI systems, they do not constitute AI systems on their own. AI models require the addition of further components, such as for example a user interface, to become AI systems. AI models are typically integrated into and form part of AI systems. This Regulation provides specific rules for general-purpose AI models and for general-purpose AI models that pose systemic risks, which should apply also when these models are integrated or form part of an AI system. It should be understood that the obligations for the providers of general-purpose AI models should apply once the general-purpose AI models are placed on the market. When the provider of a general-purpose AI model integrates an own model into its own AI system that is made available on the market or put into service, that model should be considered to be placed on the market and, therefore, the obligations in this Regulation for models should continue to apply in addition to those for AI systems. The obligations laid down for models should in any case not apply when an own model is used for purely internal processes that are not essential for providing a product or a service to third parties and the rights of natural persons are not affected. Considering their potential significantly negative effects, the general-purpose AI models with systemic risk should always be subject to the relevant obligations under this Regulation. The definition should not cover AI models used before their placing on the market for the sole purpose of research, development and prototyping activities. This is without prejudice to the obligation to comply with this Regulation when, following such activities, a model is placed on the market.

(98) Whereas the generality of a model could, inter alia, also be determined by a number of parameters, models with at least a billion of parameters and trained with a large amount of data using self-supervision at scale should be considered to display significant generality and to competently perform a wide range of distinctive tasks.

(99) Large generative AI models are a typical example for a general-purpose AI model, given that they allow for flexible generation of content, such as in the form of text, audio, images or video, that can readily accommodate a wide range of distinctive tasks.

(100) When a general-purpose AI model is integrated into or forms part of an AI system, this system should be considered to be general-purpose AI system when, due to this integration, this system has the capability to serve a variety of purposes. A general-purpose AI system can be used directly, or it may be integrated into other AI systems.

影响评估应识别部署者将按照其预期目的使用高风险人工智能系统的相关流程，并应包括系统预期使用的时间段和频率的描述，以及在特定使用情境中可能受影响的具体自然人类别和群体的描述。评估还应包括识别可能对这些个人或群体的基本权利产生影响的具体伤害风险。在进行此评估时，部署者应考虑与适当评估影响相关的信息，包括但不限于高风险人工智能系统提供者在使用说明中提供的信息。鉴于所识别的风险，部署者应确定在这些风险实际发生时应采取的措施，例如包括该特定使用情境中的治理安排，如根据使用说明进行人类监督的安排，或投诉处理和补救程序，因为这些措施可能有助于在具体用例中减轻对基本权利的风险。在进行该影响评估后，部署者应通知相关市场监督机构。在适当情况下，为收集进行影响评估所需的有关信息，高风险人工智能系统的部署者，特别是在公共部门使用人工智能系统时，可让相关利益相关方参与进行此类影响评估和设计在风险实际发生时应采取的措施，包括可能受人工智能系统影响的群体代表、独立专家和民间社会组织。欧洲人工智能办公室(人工智能办公室)应制定问卷模板，以便利合规并减轻部署者的行政负担。

(97) 通用人工智能模型的概念应明确界定，并与人工智能系统的概念区分开来，以
实现法律确定性。该定义应基于通用人工智能模型的关键功能特征，特别是通用性和胜任执行广泛不同任务的能力。这些模型通常通过各种方法(如自监督、无监督或强化学习)在大量数据上进行训练。通用人工智能模型可通过多种方式投放市场，包括通过库、应用程序编程接口(API)、直接下载或作为物理副本。这些模型可进一步修改或微调为新模型。尽管人工智能模型是人工智能系统的重要组成部分，但它们本身不构成人工智能系统。人工智能模型需要添加其他组件(例如用户界面)才能成为人工智能系统。人工智能模型通常被集成到人工智能系统中并构成其一部分。本法规对通用人工智能模型和构成系统性风险的通用人工智能模型规定了具体规则，这些规则在这些模型被集成或构成人工智能系统的一部分时也应适用。应理解为，通用人工智能模型提供者的义务应在通用人工智能模型投放市场后适用。当通用人工智能模型的提供者将自有模型集成到其投放市场或投入使用的自有人工智能系统中时，该模型应被视为已投放市场，因此，本法规对模型的义务应在人工智能系统义务之外继续适用。当自有模型仅用于纯粹内部流程，且这些流程对向第三方提供产品或服务并非必要且自然人的权利不受影响时，对模型规定的义务在任何情况下均不适用。考虑到其潜在的显著负面影响，具有系统性风险的通用人工智能模型应始终遵守本法规下的相关义务。该定义不应涵盖在投放市场之前仅用于研究、开发和原型设计活动的人工智能模型。这不影响在此类活动之后模型投放市场时遵守本法规的义务。

(98) 鉴于模型的通用性除其他外还可由若干参数确定，具有至少
十亿参数并使用大规模自监督以大量数据训练的模型，应被视为具有显著通用性，并能够胜任执行广泛的不同任务。

(99) 大型生成式人工智能模型是通用人工智能模型的典型示例，因为它们允许灵活
生成内容，例如以文本、音频、图像或视频形式，可随时适应广泛的不同任务。

(100) 当通用人工智能模型集成到人工智能系统中或构成其一部分时，该人工智能系统应被视为
通用人工智能系统，当由于此种集成，该系统具有服务于多种用途的能力时。通用人工智能系统可直接使用，也可集成到其他人工智能系统中。

(101) Providers of general-purpose AI models have a particular role and responsibility along the AI value chain, as the models they provide may form the basis for a range of downstream systems, often provided by downstream providers that necessitate a good understanding of the models and their capabilities, both to enable the integration of such models into their products, and to fulfil their obligations under this or other regulations. Therefore, proportionate transparency measures should be laid down, including the drawing up and keeping up to date of documentation, and the provision of information on the general-purpose AI model for its usage by the downstream providers. Technical documentation should be prepared and kept up to date by the general-purpose AI model provider for the purpose of making it available, upon request, to the AI Office and the national competent authorities. The minimal set of elements to be included in such documentation should be set out in specific annexes to this Regulation. The Commission should be empowered to amend those annexes by means of delegated acts in light of evolving technological developments.

(102) Software and data, including models, released under a free and open-source licence that allows them to be openly shared and where users can freely access, use, modify and redistribute them or modified versions thereof, can contribute to research and innovation in the market and can provide significant growth opportunities for the Union economy. General-purpose AI models released under free and open-source licences should be considered to ensure high levels of transparency and openness if their parameters, including the weights, the information on the model architecture, and the information on model usage are made publicly available. The licence should be considered to be free and open-source also when it allows users to run, copy, distribute, study, change and improve software and data, including models under the condition that the original provider of the model is credited, the identical or comparable terms of distribution are respected.

(103) Free and open-source AI components covers the software and data, including models and general-purpose AI models, tools, services or processes of an AI system. Free and open-source AI components can be provided through different channels, including their development on open repositories. For the purposes of this Regulation, AI components that are provided against a price or otherwise monetised, including through the provision of technical support or other services, including through a software platform, related to the AI component, or the use of personal data for reasons other than exclusively for improving the security, compatibility or interoperability of the software, with the exception of transactions between microenterprises, should not benefit from the exceptions provided to free and open-source AI components. The fact of making AI components available through open repositories should not, in itself, constitute a monetisation.

(104) The providers of general-purpose AI models that are released under a free and open-source licence, and whose parameters, including the weights, the information on the model architecture, and the information on model usage, are made publicly available should be subject to exceptions as regards the transparency-related requirements imposed on general-purpose AI models, unless they can be considered to present a systemic risk, in which case the circumstance that the model is transparent and accompanied by an open-source license should not be considered to be a sufficient reason to exclude compliance with the obligations under this Regulation. In any case, given that the release of general-purpose AI models under free and open-source licence does not necessarily reveal substantial information on the data set used for the training or fine-tuning of the model and on how compliance of copyright law was thereby ensured, the exception provided for general-purpose AI models from compliance with the transparency-related requirements should not concern the obligation to produce a summary about the content used for model training and the obligation to put in place a policy to comply with Union copyright law, in particular to identify and comply with the reservation of rights pursuant to Article 4(3) of Directive (EU) 2019/790 of the European Parliament and of the Council ([40]).

(105) General-purpose AI models, in particular large generative AI models, capable of generating text, images, and other content, present unique innovation opportunities but also challenges to artists, authors, and other creators and the way their creative content is created, distributed, used and consumed. The development and training of such models require access to vast amounts of text, images, videos and other data. Text and data mining techniques may be used extensively in this context for the retrieval and analysis of such content, which may be protected by copyright and related rights. Any use of copyright protected content requires the authorisation of the rightsholder concerned unless relevant copyright exceptions and limitations apply. Directive (EU) 2019/790 introduced exceptions and limitations allowing reproductions and extractions of works or other subject matter, for the purpose of text and data

([40]) Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (OJ L 130, 17.5.2019, p. 92).

(101) 通用人工智能模型的提供者在人工智能价值链中具有特殊的作用和责任，因为其提供的模型可能构成一系列下游系统的基础，这些系统通常由下游提供者提供，而下游提供者需要充分了解这些模型及其能力，以便将这些模型集成到其产品中，并履行本条例或其他法规规定的义务。因此，应规定相称的透明度措施，包括起草并保持文档的最新状态，以及向下游提供者提供有关通用人工智能模型的信息以供其使用。通用人工智能模型提供者应编制并保持技术文档的最新状态，以便应要求向人工智能办公室和国家主管机关提供。此类文档应包含的最低要素应在本条例的特定附件中规定。应授权委员会根据不断发展的技术进展，通过授权法案修订这些附件。

(102) 根据自由和开源许可证发布的软件和数据，包括模型，允许公开共享，用户可以自由访问、使用、修改和重新分发这些软件和数据或其修改版本，可以促进市场的研究和创新，并可为欧盟经济提供重大增长机会。根据自由和开源许可证发布的通用人工智能模型，如果其参数(包括权重、模型架构信息和模型使用信息)公开可用，则应被视为确保高水平的透明度和开放性。当许可证允许用户运行、复制、分发、研究、更改和改进软件和数据(包括模型)，条件是注明模型的原始提供者、遵守相同或可比的分发条款时，该许可证也应被视为自由和开源许可证。

(103) 自由和开源人工智能组件涵盖人工智能系统的软件和数据，包括模型和通用人工智能模型、工具、服务或流程。自由和开源人工智能组件可通过不同渠道提供，包括在开放存储库上进行开发。就本条例而言，以付费或其他方式货币化提供的人工智能组件，包括通过与人工智能组件相关的技术支持或其他服务(包括通过软件平台)提供，或出于非仅为改善软件安全性、兼容性或互操作性的目的使用个人数据，但微型企业之间的交易除外，不应受益于向自由和开源人工智能组件提供的例外。通过开放存储库提供人工智能组件这一事实本身不应构成货币化。

(104) 以自由和开源许可证发布、且其参数(包括权重、模型架构信息和模型使用信息)已公开的通用人工智能模型的提供者，应当就施加于通用人工智能模型的透明度相关要求享有例外，除非可被认为构成系统性风险，在此情况下，模型具有透明度并附有开源许可证这一情形不应被视为排除遵守本条例义务的充分理由。无论如何，鉴于以自由和开源许可证发布通用人工智能模型并不必然揭示用于模型训练或微调的数据集的大量信息，也不必然揭示如何由此确保遵守版权法，为通用人工智能模型规定的免于遵守透明度相关要求的例外不应涉及制作关于用于模型训练的内容摘要的义务，也不应涉及制定遵守欧盟版权法(特别是依据欧洲议会和理事会指令(EU) 2019/790第4(3)条识别并遵守权利保留)的政策的义务。

(105) 通用人工智能模型，特别是能够生成文本、图像和其他内容的大型生成式人工智能模型，为艺术家、作者和其他创作者及其创意内容的创作、分发、使用和消费方式带来了独特的创新机遇，但也带来了挑战。此类模型的开发和训练需要访问大量文本、图像、视频和其他数据。在此背景下，文本和数据挖掘技术可能被广泛用于检索和分析此类内容，这些内容可能受版权和相关权利保护。任何使用受版权保护的内容都需要相关权利持有人的授权，除非适用的版权例外和限制。指令(EU) 2019/790引入了例外和限制，允许为文本和数据目的复制和提取作品或其他客体

(40) 欧洲议会和理事会2019年4月17日关于数字单一市场版权及相关权利并修订第96/9/EC号和第2001/29/EC号指令的第(EU) 2019/790号指令(OJ L 130, 17.5.2019, p.92)。

mining, under certain conditions. Under these rules, rightsholders may choose to reserve their rights over their works or other subject matter to prevent text and data mining, unless this is done for the purposes of scientific research. Where the rights to opt out has been expressly reserved in an appropriate manner, providers of general-purpose AI models need to obtain an authorisation from rightsholders if they want to carry out text and data mining over such works.

(106) Providers that place general-purpose AI models on the Union market should ensure compliance with the relevant obligations in this Regulation. To that end, providers of general-purpose AI models should put in place a policy to comply with Union law on copyright and related rights, in particular to identify and comply with the reservation of rights expressed by rightsholders pursuant to Article 4(3) of Directive (EU) 2019/790. Any provider placing a general-purpose AI model on the Union market should comply with this obligation, regardless of the jurisdiction in which the copyright-relevant acts underpinning the training of those general-purpose AI models take place. This is necessary to ensure a level playing field among providers of general-purpose AI models where no provider should be able to gain a competitive advantage in the Union market by applying lower copyright standards than those provided in the Union.

(107) In order to increase transparency on the data that is used in the pre-training and training of general-purpose AI models, including text and data protected by copyright law, it is adequate that providers of such models draw up and make publicly available a sufficiently detailed summary of the content used for training the general-purpose AI model. While taking into due account the need to protect trade secrets and confidential business information, this summary should be generally comprehensive in its scope instead of technically detailed to facilitate parties with legitimate interests, including copyright holders, to exercise and enforce their rights under Union law, for example by listing the main data collections or sets that went into training the model, such as large private or public databases or data archives, and by providing a narrative explanation about other data sources used. It is appropriate for the AI Office to provide a template for the summary, which should be simple, effective, and allow the provider to provide the required summary in narrative form.

(108) With regard to the obligations imposed on providers of general-purpose AI models to put in place a policy to comply with Union copyright law and make publicly available a summary of the content used for the training, the AI Office should monitor whether the provider has fulfilled those obligations without verifying or proceeding to a work-by-work assessment of the training data in terms of copyright compliance. This Regulation does not affect the enforcement of copyright rules as provided for under Union law.

(109) Compliance with the obligations applicable to the providers of general-purpose AI models should be commensurate and proportionate to the type of model provider, excluding the need for compliance for persons who develop or use models for non-professional or scientific research purposes, who should nevertheless be encouraged to voluntarily comply with these requirements. Without prejudice to Union copyright law, compliance with those obligations should take due account of the size of the provider and allow simplified ways of compliance for SMEs, including start-ups, that should not represent an excessive cost and not discourage the use of such models. In the case of a modification or fine-tuning of a model, the obligations for providers of general-purpose AI models should be limited to that modification or fine-tuning, for example by complementing the already existing technical documentation with information on the modifications, including new training data sources, as a means to comply with the value chain obligations provided in this Regulation.

(110) General-purpose AI models could pose systemic risks which include, but are not limited to, any actual or reasonably foreseeable negative effects in relation to major accidents, disruptions of critical sectors and serious consequences to public health and safety; any actual or reasonably foreseeable negative effects on democratic processes, public and economic security; the dissemination of illegal, false, or discriminatory content. Systemic risks should be understood to increase with model capabilities and model reach, can arise along the entire lifecycle of the model, and are influenced by conditions of misuse, model reliability, model fairness and model security, the level of autonomy of

挖掘，在某些条件下。根据这些规则，权利持有人可选择保留其对作品或其他标的物的权利，以防止文本和数据挖掘，除非是为科学研究目的而进行。在以适当方式明确保留选择退出权的情况下，通用人工智能模型提供者如欲对此类作品进行文本和数据挖掘，需获得权利持有人的授权。

(106) 在欧盟市场投放通用人工智能模型的提供者应确保遵守本条例的相关义务。为此，通用人工智能模型的提供者应制定政策，以遵守欧盟关于版权及相关权利的法律，特别是识别并遵守权利持有人依据Directive (EU) 2019/790第4(3)条所表达的权利保留。任何在欧盟市场投放通用人工智能模型的提供者均应遵守该义务，无论支撑这些通用人工智能模型训练的版权相关行为发生在哪个司法管辖区。这对于确保通用人工智能模型提供者之间的公平竞争环境是必要的，任何提供者都不应能够通过适用低于欧盟所规定标准的版权标准而在欧盟市场获得竞争优势。

(107) 为提高用于通用人工智能模型预训练和训练的数据(包括受版权法保护的文本和数据)的透明度，此类模型的提供者应编制并公开提供一份关于用于训练通用人工智能模型内容的足够详细的摘要。在适当考虑保护商业秘密和保密商业信息需要的同时，该摘要应在其范围上总体全面，而非技术上的详尽，以便包括版权持有人在内的有合法利益的各方能够行使和执行其在欧盟法律下的权利，例如列出用于训练模型的主要数据集合或数据集，如大型私人或公共数据库或数据档案，并对所使用的其他数据来源提供叙述性说明。人工智能办公室宜为该摘要提供模板，该模板应简单、有效，并允许提供者以叙述形式提供所需摘要。

(108) 关于对通用人工智能模型提供者施加的制定遵守欧盟版权法政策并公开提供用于训练内容摘要的义务，人工智能办公室应监督提供者是否履行了这些义务，而不对训练数据在版权合规方面进行核实或逐件评估。本条例不影响欧盟法律所规定的版权规则的执行。

(109) 对通用人工智能模型提供者适用义务的遵守应与其模型提供者类型相称且成比例，排除为非专业或科学研究目的开发或使用模型的人员的合规需要，但仍应鼓励其自愿遵守这些要求。在不影响欧盟版权法的情况下，遵守这些义务应适当考虑提供者的规模，并允许包括初创企业在内的SME采用简化合规方式，这种方式不应构成过高成本，也不应阻碍对此类模型的使用。在对模型进行修改或微调的情况下，通用人工智能模型提供者的义务应限于该修改或微调，例如通过以关于修改的信息(包括新的训练数据来源)补充现有技术文档，作为遵守本条例所规定价值链义务的一种方式。

(110) 通用人工智能模型可能构成系统性风险，包括但不限于：与重大事故、关键部门中断以及对公共健康和安全造成严重后果相关的任何实际或合理可预见的负面影响；对民主进程、公共和经济安全的任何实际或合理可预见的负面影响；非法、虚假或歧视性内容的传播。系统性风险应被理解为随模型能力和模型覆盖范围而增加，可能在模型的整个生命周期中出现，并受滥用条件、模型可靠性、模型公平性和模型安全性、自主性水平的影响

the model, its access to tools, novel or combined modalities, release and distribution strategies, the potential to remove guardrails and other factors. In particular, international approaches have so far identified the need to pay attention to risks from potential intentional misuse or unintended issues of control relating to alignment with human intent; chemical, biological, radiological, and nuclear risks, such as the ways in which barriers to entry can be lowered, including for weapons development, design acquisition, or use; offensive cyber capabilities, such as the ways in vulnerability discovery, exploitation, or operational use can be enabled; the effects of interaction and tool use, including for example the capacity to control physical systems and interfere with critical infrastructure; risks from models of making copies of themselves or 'self-replicating' or training other models; the ways in which models can give rise to harmful bias and discrimination with risks to individuals, communities or societies; the facilitation of disinformation or harming privacy with threats to democratic values and human rights; risk that a particular event could lead to a chain reaction with considerable negative effects that could affect up to an entire city, an entire domain activity or an entire community.

(111) It is appropriate to establish a methodology for the classification of general-purpose AI models as general-purpose AI model with systemic risks. Since systemic risks result from particularly high capabilities, a general-purpose AI model should be considered to present systemic risks if it has high-impact capabilities, evaluated on the basis of appropriate technical tools and methodologies, or significant impact on the internal market due to its reach. High-impact capabilities in general-purpose AI models means capabilities that match or exceed the capabilities recorded in the most advanced general-purpose AI models. The full range of capabilities in a model could be better understood after its placing on the market or when deployers interact with the model. According to the state of the art at the time of entry into force of this Regulation, the cumulative amount of computation used for the training of the general-purpose AI model measured in floating point operations is one of the relevant approximations for model capabilities. The cumulative amount of computation used for training includes the computation used across the activities and methods that are intended to enhance the capabilities of the model prior to deployment, such as pre-training, synthetic data generation and fine-tuning. Therefore, an initial threshold of floating point operations should be set, which, if met by a general-purpose AI model, leads to a presumption that the model is a general-purpose AI model with systemic risks. This threshold should be adjusted over time to reflect technological and industrial changes, such as algorithmic improvements or increased hardware efficiency, and should be supplemented with benchmarks and indicators for model capability. To inform this, the AI Office should engage with the scientific community, industry, civil society and other experts. Thresholds, as well as tools and benchmarks for the assessment of high-impact capabilities, should be strong predictors of generality, its capabilities and associated systemic risk of general-purpose AI models, and could take into account the way the model will be placed on the market or the number of users it may affect. To complement this system, there should be a possibility for the Commission to take individual decisions designating a general-purpose AI model as a general-purpose AI model with systemic risk if it is found that such model has capabilities or an impact equivalent to those captured by the set threshold. That decision should be taken on the basis of an overall assessment of the criteria for the designation of a general-purpose AI model with systemic risk set out in an annex to this Regulation, such as quality or size of the training data set, number of business and end users, its input and output modalities, its level of autonomy and scalability, or the tools it has access to. Upon a reasoned request of a provider whose model has been designated as a general-purpose AI model with systemic risk, the Commission should take the request into account and may decide to reassess whether the general-purpose AI model can still be considered to present systemic risks.

(112) It is also necessary to clarify a procedure for the classification of a general-purpose AI model with systemic risks. A general-purpose AI model that meets the applicable threshold for high-impact capabilities should be presumed to be a general-purpose AI models with systemic risk. The provider should notify the AI Office at the latest two weeks after the requirements are met or it becomes known that a general-purpose AI model will meet the requirements that lead to the presumption. This is especially relevant in relation to the threshold of floating point operations because training of general-purpose AI models takes considerable planning which includes the upfront allocation of compute resources and, therefore, providers of general-purpose AI models are able to know if their model would meet the threshold before the training is completed. In the context of that notification, the provider should be able to demonstrate that, because of its specific characteristics, a general-purpose AI model exceptionally does not present systemic risks, and that it thus should not be classified as a general-purpose AI model with systemic risks. That information is valuable for the AI Office to anticipate the placing on the market of general-purpose AI models with systemic risks and the providers can start to engage with the AI Office early on. That information is especially

模型、其获取工具的能力、新颖或组合模态、发布与分发策略、移除防护措施的可能性以及其他因素。特别是，国际方法迄今已识别出需要关注以下风险：与人类意图对齐相关的潜在故意滥用或意外控制问题；化学、生物、放射性及核风险，例如降低准入门槛的方式，包括用于武器开发、设计获取或使用；攻击性网络能力，例如漏洞发现、利用或作战使用被赋能的方式；交互与工具使用的效应，包括例如控制物理系统和干扰关键基础设施的能力；模型自我复制或"自我复制"或训练其他模型的风险；模型可能引发有害偏见和歧视，对个人、社区或社会构成风险；助长虚假信息或损害隐私，对民主价值观和人权构成威胁；特定事件可能引发连锁反应并产生重大负面影响，可能波及整个城市、整个领域活动或整个社区的风险。

(111) 宜建立一种将通用人工智能模型归类为通用

具有系统性风险的人工智能模型。由于系统性风险源于特别高的能力，如果通用人工智能模型具有高影响力能力(基于适当的技术工具和方法进行评估)，或因其覆盖范围而对内部市场产生重大影响，则应被视为具有系统性风险。通用人工智能模型中的高影响力能力是指匹配或超过最先进通用人工智能模型中记录的能力。模型的全谱能力可在其投放市场后或部署者与模型交互时得到更好的理解。根据本 Regulation 生效时的现有技术水平，以浮点运算衡量的用于训练通用人工智能模型的累计算力是模型能力的相关近似指标之一。用于训练的累计算力包括在部署前旨在增强模型能力的活动和方法中所使用的算力，例如预训练、合成数据生成和微调。因此，应设定一个初始浮点运算阈值，如果通用人工智能模型达到该阈值，则推定该模型为具有系统性风险的通用人工智能模型。该阈值应随时间调整以反映技术和产业变化，例如算法改进或硬件效率提高，并应辅以模型能力的基准和指标。为此，人工智能办公室应与科学界、产业界、民间社会和其他专家接触。阈值以及用于评估高影响力能力的工具和基准应是通用人工智能模型的通用性、其能力及相关系统性风险的强预测指标，并可考虑模型投放市场的方式或其可能影响的用户数量。为补充该制度，如果发现通用人工智能模型具有与设定阈值所涵盖的能力或影响相当的能力或影响，委员会应有可能作出个别决定，将该通用人工智能模型指定为具有系统性风险的通用人工智能模型。该决定应基于对本 Regulation 附件中规定的具有系统性风险的通用人工智能模型指定标准的总体评估，例如训练数据集的质量或规模、商业和最终用户数量、其输入和输出模态、其自主性和可扩展性水平，或其可获取的工具。应其模型已被指定为具有系统性风险的通用人工智能模型的提供者的合理请求，委员会应考虑该请求，并可决定重新评估该通用人工智能模型是否仍可被视为具有系统性风险。

(112) 还有必要澄清具有系统性风险的通用人工智能模型分类程序。

符合高影响力能力适用阈值的通用人工智能模型应被推定为具有系统性风险的通用人工智能模型。提供者应在满足要求后最迟两周内，或在得知通用人工智能模型将满足导致推定的要求时，通知人工智能办公室。这与浮点运算阈值尤其相关，因为通用人工智能模型的训练需要大量规划，包括前期算力资源分配，因此通用人工智能模型的提供者能够在训练完成前知道其模型是否将达到阈值。在该通知的背景下，提供者应能够证明，由于其特定特征，通用人工智能模型例外地不具有系统性风险，因此不应被归类为具有系统性风险的通用人工智能模型。该信息对人工智能办公室预测具有系统性风险的通用人工智能模型的投放市场很有价值，提供者可以尽早与人工智能办公室接触。该信息尤其

important with regard to general-purpose AI models that are planned to be released as open-source, given that, after the open-source model release, necessary measures to ensure compliance with the obligations under this Regulation may be more difficult to implement.

(113) If the Commission becomes aware of the fact that a general-purpose AI model meets the requirements to classify as a general-purpose AI model with systemic risk, which previously had either not been known or of which the relevant provider has failed to notify the Commission, the Commission should be empowered to designate it so. A system of qualified alerts should ensure that the AI Office is made aware by the scientific panel of general-purpose AI models that should possibly be classified as general-purpose AI models with systemic risk, in addition to the monitoring activities of the AI Office.

(114) The providers of general-purpose AI models presenting systemic risks should be subject, in addition to the obligations provided for providers of general-purpose AI models, to obligations aimed at identifying and mitigating those risks and ensuring an adequate level of cybersecurity protection, regardless of whether it is provided as a standalone model or embedded in an AI system or a product. To achieve those objectives, this Regulation should require providers to perform the necessary model evaluations, in particular prior to its first placing on the market, including conducting and documenting adversarial testing of models, also, as appropriate, through internal or independent external testing. In addition, providers of general-purpose AI models with systemic risks should continuously assess and mitigate systemic risks, including for example by putting in place risk-management policies, such as accountability and governance processes, implementing post-market monitoring, taking appropriate measures along the entire model's lifecycle and cooperating with relevant actors along the AI value chain.

(115) Providers of general-purpose AI models with systemic risks should assess and mitigate possible systemic risks. If, despite efforts to identify and prevent risks related to a general-purpose AI model that may present systemic risks, the development or use of the model causes a serious incident, the general-purpose AI model provider should without undue delay keep track of the incident and report any relevant information and possible corrective measures to the Commission and national competent authorities. Furthermore, providers should ensure an adequate level of cybersecurity protection for the model and its physical infrastructure, if appropriate, along the entire model lifecycle. Cybersecurity protection related to systemic risks associated with malicious use or attacks should duly consider accidental model leakage, unauthorised releases, circumvention of safety measures, and defence against cyberattacks, unauthorised access or model theft. That protection could be facilitated by securing model weights, algorithms, servers, and data sets, such as through operational security measures for information security, specific cybersecurity policies, adequate technical and established solutions, and cyber and physical access controls, appropriate to the relevant circumstances and the risks involved.

(116) The AI Office should encourage and facilitate the drawing up, review and adaptation of codes of practice, taking into account international approaches. All providers of general-purpose AI models could be invited to participate. To ensure that the codes of practice reflect the state of the art and duly take into account a diverse set of perspectives, the AI Office should collaborate with relevant national competent authorities, and could, where appropriate, consult with civil society organisations and other relevant stakeholders and experts, including the Scientific Panel, for the drawing up of such codes. Codes of practice should cover obligations for providers of general-purpose AI models and of general-purpose AI models presenting systemic risks. In addition, as regards systemic risks, codes of practice should help to establish a risk taxonomy of the type and nature of the systemic risks at Union level, including their sources. Codes of practice should also be focused on specific risk assessment and mitigation measures.

(117) The codes of practice should represent a central tool for the proper compliance with the obligations provided for under this Regulation for providers of general-purpose AI models. Providers should be able to rely on codes of practice to demonstrate compliance with the obligations. By means of implementing acts, the Commission may decide to approve a code of practice and give it a general validity within the Union, or, alternatively, to provide common rules for the implementation of the relevant obligations, if, by the time this Regulation becomes applicable, a code of practice cannot be finalised or is not deemed adequate by the AI Office. Once a harmonised standard is

对于计划作为开源发布的通用人工智能模型尤为重要，因为在开源模型发布后，确保遵守本条例义务的必要措施可能更难实施。

(113) 如果委员会知悉某一通用人工智能模型符合被归类为具有系统性风险的通用人工智能模型的要求，而此前该情况不为人知或相关提供者未通知委员会，则委员会应有权将其指定为具有系统性风险的通用人工智能模型。合格警报系统应确保除人工智能办公室的监测活动外，科学小组还向人工智能办公室告知可能应被归类为具有系统性风险的通用人工智能模型。

(114) 具有系统性风险的通用人工智能模型的提供者，除适用于通用人工智能模型提供者的义务外，还应承担旨在识别和缓解这些风险并确保适当网络安全保护水平的义务，无论其是作为独立模型提供还是嵌入人工智能系统或产品中。为实现这些目标，本 Regulation 应要求提供者进行必要的模型评估，特别是在其首次投放市场之前，包括对模型进行对抗性测试并记录，也可酌情通过内部或独立外部测试进行。此外，具有系统性风险的通用人工智能模型的提供者应持续评估和缓解系统性风险，包括例如制定风险管理政策，如问责和治理流程，实施上市后监测，在模型整个生命周期采取适当措施，并与人工智能价值链上的相关行为者合作。

(115) 具有系统性风险的通用人工智能模型的提供者应当评估并缓解可能的系统性风险。如果尽管已努力识别和预防与可能呈现系统性风险的通用人工智能模型相关的风险，该模型的开发或使用仍导致严重事件，则通用人工智能模型提供者应当毫不迟延地跟踪该事件，并向委员会和国家主管机关报告任何相关信息和可能的纠正措施。此外，提供者应当在整个模型生命周期内，酌情确保为该模型及其物理基础设施提供适当水平的网络安全保护。与恶意使用或攻击相关的系统性风险的网络安全保护，应当适当考虑意外的模型泄露、未经授权的发布、规避安全措施，以及对网络攻击、未经授权访问或模型窃取的防御。此类保护可通过保护模型权重、算法、服务器和数据集来促进，例如通过信息安全的操作安全措施、具体的网络安全政策、适当的技术和成熟解决方案，以及网络和物理访问控制，并与相关情况和所涉风险相适应。

(116) 人工智能办公室应当鼓励和促进行为准则的制定、审查和调整，同时考虑国际做法。可邀请所有通用人工智能模型的提供者参与。为确保行为准则反映最新技术水平并适当考虑多样化的观点，人工智能办公室应当与相关国家主管机关合作，并可酌情与民间社会组织及其他相关利益相关者和专家(包括科学小组)协商，以制定此类准则。行为准则应当涵盖通用人工智能模型提供者以及呈现系统性风险的通用人工智能模型提供者的义务。此外，关于系统性风险，行为准则应当有助于在联盟层面建立关于系统性风险类型和性质的风险分类体系，包括其来源。行为准则还应当侧重于具体的风险评估和缓解措施。

(117) 行为准则应当成为通用人工智能模型提供者妥善遵守本条例所规定义务的核心工具。提供者应当能够依据行为准则证明其遵守了义务。通过实施法案，如果在本条例适用之时行为准则无法最终确定或未被人工智能办公室认为适当，委员会可决定批准行为准则并赋予其在联盟内的一般效力，或者，作为替代，为相关义务的实施提供共同规则。一旦协调标准

published and assessed as suitable to cover the relevant obligations by the AI Office, compliance with a European harmonised standard should grant providers the presumption of conformity. Providers of general-purpose AI models should furthermore be able to demonstrate compliance using alternative adequate means, if codes of practice or harmonised standards are not available, or they choose not to rely on those.

(118) This Regulation regulates AI systems and AI models by imposing certain requirements and obligations for relevant market actors that are placing them on the market, putting into service or use in the Union, thereby complementing obligations for providers of intermediary services that embed such systems or models into their services regulated by Regulation (EU) 2022/2065. To the extent that such systems or models are embedded into designated very large online platforms or very large online search engines, they are subject to the risk-management framework provided for in Regulation (EU) 2022/2065. Consequently, the corresponding obligations of this Regulation should be presumed to be fulfilled, unless significant systemic risks not covered by Regulation (EU) 2022/2065 emerge and are identified in such models. Within this framework, providers of very large online platforms and very large online search engines are obliged to assess potential systemic risks stemming from the design, functioning and use of their services, including how the design of algorithmic systems used in the service may contribute to such risks, as well as systemic risks stemming from potential misuses. Those providers are also obliged to take appropriate mitigating measures in observance of fundamental rights.

(119) Considering the quick pace of innovation and the technological evolution of digital services in scope of different instruments of Union law in particular having in mind the usage and the perception of their recipients, the AI systems subject to this Regulation may be provided as intermediary services or parts thereof within the meaning of Regulation (EU) 2022/2065, which should be interpreted in a technology-neutral manner. For example, AI systems may be used to provide online search engines, in particular, to the extent that an AI system such as an online chatbot performs searches of, in principle, all websites, then incorporates the results into its existing knowledge and uses the updated knowledge to generate a single output that combines different sources of information.

(120) Furthermore, obligations placed on providers and deployers of certain AI systems in this Regulation to enable the detection and disclosure that the outputs of those systems are artificially generated or manipulated are particularly relevant to facilitate the effective implementation of Regulation (EU) 2022/2065. This applies in particular as regards the obligations of providers of very large online platforms or very large online search engines to identify and mitigate systemic risks that may arise from the dissemination of content that has been artificially generated or manipulated, in particular risk of the actual or foreseeable negative effects on democratic processes, civic discourse and electoral processes, including through disinformation.

(121) Standardisation should play a key role to provide technical solutions to providers to ensure compliance with this Regulation, in line with the state of the art, to promote innovation as well as competitiveness and growth in the single market. Compliance with harmonised standards as defined in Article 2, point (1)(c), of Regulation (EU) No 1025/2012 of the European Parliament and of the Council ([41]), which are normally expected to reflect the state of the art, should be a means for providers to demonstrate conformity with the requirements of this Regulation. A balanced representation of interests involving all relevant stakeholders in the development of standards, in particular SMEs, consumer organisations and environmental and social stakeholders in accordance with Articles 5 and 6 of Regulation (EU) No 1025/2012 should therefore be encouraged. In order to facilitate compliance, the standardisation requests should be issued by the Commission without undue delay. When preparing the standardisation request, the Commission should consult the advisory forum and the Board in order to collect relevant expertise. However, in the absence of relevant references to harmonised standards, the Commission should be able to establish, via implementing acts, and after consultation of the advisory forum, common specifications for certain requirements under this Regulation. The common specification should be an exceptional fall back solution to facilitate the provider's obligation to comply with the requirements of this Regulation, when the standardisation request has not been accepted by any of the European standardisation organisations, or when the relevant harmonised standards insufficiently address fundamental rights concerns, or when the harmonised standards do not comply with the request, or when there are delays in the adoption of an appropriate harmonised standard. Where such a delay in the adoption of a harmonised standard is due to the technical complexity of that standard, this should

([41]) Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (OJ L 316, 14.11.2012, p. 12).

由人工智能办公室发布并评估为适合涵盖相关义务的，遵守欧洲协调标准应给予提供者符合性推定。通用人工智能模型提供者还应能够在行为准则或协调标准不可用，或他们选择不依赖这些准则或标准时，使用替代的适当方式证明合规性。

(118) 本条例通过对此类系统或模型投放市场、在联盟内投入使用或使用的相关市场参与者施加某些要求和义务，对人工智能系统和人工智能模型进行规范，从而补充将此类系统或模型嵌入其受Regulation(EU) 2022/2065规范的服务中的中间服务提供者的义务。在此类系统或模型被嵌入指定的超大型在线平台或超大型在线搜索引擎的范围内，它们受Regulation(EU) 2022/2065所规定的风险管理框架约束。因此，除非此类模型中出现并识别出Regulation(EU) 2022/2065未涵盖的重大系统性风险，否则应当推定本条例的相应义务已得到履行。在此框架内，超大型在线平台和超大型在线搜索引擎的提供者有义务评估因其服务的设计、运行和使用而产生的潜在系统性风险，包括服务中所使用的算法系统的设计如何可能促成此类风险，以及因潜在滥用而产生的系统性风险。这些提供者还有义务在遵守基本权利的前提下采取适当的缓解措施。

(119) 考虑到联盟法律不同文书范围内数字服务的创新和技术演进的快速步伐，特别是考虑到其接收者的使用和认知，受本条例约束的人工智能系统可以作为Regulation(EU) 2022/2065含义内的中间服务或其组成部分提供，对此应当以技术中立的方式加以解释。例如，人工智能系统可用于提供在线搜索引擎，特别是在诸如在线聊天机器人等人工智能系统原则上搜索所有网站、然后将结果纳入其现有知识并利用更新后的知识生成结合不同信息来源的单一输出的情况下。

(120) 此外，本条例对某些人工智能系统的提供者和部署者施加的、旨在能够检测和披露这些系统的输出系人工生成或操纵的义务，对于促进(EU) 2022/2065号条例的有效实施尤为相关。这尤其适用于超大型在线平台或超大型在线搜索引擎的提供者识别和缓解因传播人工生成或操纵的内容而可能产生的系统性风险的义务，特别是对民主进程、公民话语和选举进程产生实际或可预见的负面影响的危险，包括通过虚假信息产生的风险。

(121) 标准化应发挥关键作用，为提供者提供技术解决方案，以确保按照最新技术水平遵守本条例，促进创新以及单一市场中的竞争力和增长。遵守欧洲议会和理事会(EU) No 1025/2012号条例(41)第2条第(1)款(c)项所定义的协调标准(通常预期反映最新技术水平)，应成为提供者证明符合本条例要求的一种手段。因此，应鼓励根据(EU) No 1025/2012号条例第5条和第6条，在标准制定过程中实现所有相关利益攸关方的利益平衡代表，特别是中小企业、消费者组织以及环境和社会利益攸关方。为促进合规，委员会应毫不迟延地发布标准化请求。在准备标准化请求时，委员会应咨询咨询论坛和委员会，以收集相关专业知识。然而，在缺乏相关协调标准引用的情况下，委员会应能够通过实施法案，并在咨询咨询论坛后，为本条例的某些要求制定共同规范。当标准化请求未被任何欧洲标准化组织接受时，或当相关协调标准未能充分解决基本权利关切时，或当协调标准不符合请求时，或当适当协调标准的通过出现延迟时，共同规范应作为促进提供者遵守本条例要求义务的例外性后备解决方案。当协调标准的通过出现此类延迟是由于该标准的技术复杂性时，这应

(41) 欧洲议会和理事会2012年10月25日关于欧洲标准化的(EU) No 1025/2012号条例，修订理事会第89/686/EEC号和第93/15/EEC号指令以及欧洲议会和理事会第94/9/EC号、第94/25/EC号、第95/16/EC号、第97/23/EC号、第98/34/EC号、第2004/22/EC号、第2007/23/EC号、第2009/23/EC号和第2009/105/EC号指令，并废止理事会第87/95/EEC号决定和欧洲议会和理事会第1673/2006/EC号决定(OJ L 316, 14.11.2012, p.12)。

be considered by the Commission before contemplating the establishment of common specifications. When developing common specifications, the Commission is encouraged to cooperate with international partners and international standardisation bodies.

(122) It is appropriate that, without prejudice to the use of harmonised standards and common specifications, providers of a high-risk AI system that has been trained and tested on data reflecting the specific geographical, behavioural, contextual or functional setting within which the AI system is intended to be used, should be presumed to comply with the relevant measure provided for under the requirement on data governance set out in this Regulation. Without prejudice to the requirements related to robustness and accuracy set out in this Regulation, in accordance with Article 54(3) of Regulation (EU) 2019/881, high-risk AI systems that have been certified or for which a statement of conformity has been issued under a cybersecurity scheme pursuant to that Regulation and the references of which have been published in the *Official Journal of the European Union* should be presumed to comply with the cybersecurity requirement of this Regulation in so far as the cybersecurity certificate or statement of conformity or parts thereof cover the cybersecurity requirement of this Regulation. This remains without prejudice to the voluntary nature of that cybersecurity scheme.

(123) In order to ensure a high level of trustworthiness of high-risk AI systems, those systems should be subject to a conformity assessment prior to their placing on the market or putting into service.

(124) It is appropriate that, in order to minimise the burden on operators and avoid any possible duplication, for high-risk AI systems related to products which are covered by existing Union harmonisation legislation based on the New Legislative Framework, the compliance of those AI systems with the requirements of this Regulation should be assessed as part of the conformity assessment already provided for in that law. The applicability of the requirements of this Regulation should thus not affect the specific logic, methodology or general structure of conformity assessment under the relevant Union harmonisation legislation.

(125) Given the complexity of high-risk AI systems and the risks that are associated with them, it is important to develop an adequate conformity assessment procedure for high-risk AI systems involving notified bodies, so-called third party conformity assessment. However, given the current experience of professional pre-market certifiers in the field of product safety and the different nature of risks involved, it is appropriate to limit, at least in an initial phase of application of this Regulation, the scope of application of third-party conformity assessment for high-risk AI systems other than those related to products. Therefore, the conformity assessment of such systems should be carried out as a general rule by the provider under its own responsibility, with the only exception of AI systems intended to be used for biometrics.

(126) In order to carry out third-party conformity assessments when so required, notified bodies should be notified under this Regulation by the national competent authorities, provided that they comply with a set of requirements, in particular on independence, competence, absence of conflicts of interests and suitable cybersecurity requirements. Notification of those bodies should be sent by national competent authorities to the Commission and the other Member States by means of the electronic notification tool developed and managed by the Commission pursuant to Article R23 of Annex I to Decision No 768/2008/EC.

(127) In line with Union commitments under the World Trade Organization Agreement on Technical Barriers to Trade, it is adequate to facilitate the mutual recognition of conformity assessment results produced by competent conformity assessment bodies, independent of the territory in which they are established, provided that those conformity assessment bodies established under the law of a third country meet the applicable requirements of this Regulation and the Union has concluded an agreement to that extent. In this context, the Commission should actively explore possible international instruments for that purpose and in particular pursue the conclusion of mutual recognition agreements with third countries.

(128) In line with the commonly established notion of substantial modification for products regulated by Union harmonisation legislation, it is appropriate that whenever a change occurs which may affect the compliance of a high-risk AI system with this Regulation (e.g. change of operating system or software architecture), or when the intended purpose of the system changes, that AI system should be considered to be a new AI system which should undergo a new conformity assessment. However, changes occurring to the algorithm and the performance of AI systems which continue to 'learn' after being placed on the market or put into service, namely automatically adapting how functions are carried out, should not constitute a substantial modification, provided that those changes have been pre-determined by the provider and assessed at the moment of the conformity assessment.

由委员会在考虑制定通用规范之前予以考虑。在制定通用规范时，鼓励委员会与国际伙伴和国际标准化机构合作。

(122) 在不影响使用协调标准和共同规范的情况下，对于已在反映人工智能系统预期使用所在特定地理、行为、情境或功能设定的数据上接受训练和测试的高风险人工智能系统，其提供者应被推定符合本条例所规定的数据治理要求下的相关措施，这是适当的。在不影响本条例所规定的稳健性和准确性相关要求的情况下，根据(EU) 2019/881号条例第54条第(3)款，已根据该条例的网络安全计划获得认证或已获发符合性声明、且其引用已在欧盟官方公报上公布的高风险人工智能系统，应被推定符合本条例的网络安全要求，前提是该网络安全证书或符合性声明或其部分涵盖本条例的网络安全要求。这不妨碍该网络安全计划的自愿性质。

(123) 为确保高风险人工智能系统的高度可信性，这些系统应在投放市场或投入使用前接受合格评定。

(124) 为尽量减少运营者的负担并避免任何可能的重复，对于与基于新立法框架的现有欧盟协调立法所涵盖产品相关的高风险人工智能系统，这些人工智能系统对本条例要求的合规性应作为该法律已规定的合格评定的一部分进行评估，这是适当的。因此，本条例要求的适用不应影响相关欧盟协调立法下合格评定的特定逻辑、方法或总体结构。

(125) 鉴于高风险人工智能系统的复杂性及其相关风险，为高风险人工智能系统制定涉及公告机构的适当合格评定程序(即所谓的第三方合格评定)十分重要。然而，鉴于产品安全领域专业上市前认证机构当前的经验以及所涉风险的不同性质，至少在本条例适用的初始阶段，宜将第三方合格评定对高风险人工智能系统的适用范围限制在除与产品相关的高风险人工智能系统之外的高风险人工智能系统。因此，此类系统的合格评定应作为一般规则由提供者在其自身责任下进行，唯一例外是拟用于生物识别的人工智能系统。

(126) 为在需要时开展第三方合格评定，公告机构应由国家主管机关依据本条例予以公告，前提是其符合一系列要求，特别是关于独立性、能力、无利益冲突以及适当的网络安全要求。国家主管机关应通过委员会依据第768/2008/EC号决定附件一第R23条开发并管理的电子通知工具，向委员会和其他成员国发送对这些机构的公告。

(127) 根据欧盟在世界贸易组织《技术性贸易壁垒协定》下的承诺，宜促进由合格评定机构出具的合格评定结果的互认，而不论这些机构设立于何地，前提是依据第三国法律设立的该等合格评定机构符合本条例的适用要求，且欧盟已就此缔结协定。在此背景下，委员会应积极探讨为此目的可能的国际文书，特别是争取与第三国缔结互认协定。

(128) 根据欧盟协调立法所监管产品实质性修改的通行既定概念，宜规定：凡发生可能影响高风险人工智能系统对本条例合规性的变更(例如操作系统或软件架构的变更)，或系统的预期目的发生变化时，该人工智能系统应被视为新的AI系统，应接受新的合格评定。然而，对于在投放市场或投入使用后继续"学习"的人工智能系统，即自动调整功能执行方式者，其算法和性能所发生的变更不应构成实质性修改，前提是这些变更已由提供者预先确定并在合格评定之时予以评估。

(129) High-risk AI systems should bear the CE marking to indicate their conformity with this Regulation so that they can move freely within the internal market. For high-risk AI systems embedded in a product, a physical CE marking should be affixed, and may be complemented by a digital CE marking. For high-risk AI systems only provided digitally, a digital CE marking should be used. Member States should not create unjustified obstacles to the placing on the market or the putting into service of high-risk AI systems that comply with the requirements laid down in this Regulation and bear the CE marking.

(130) Under certain conditions, rapid availability of innovative technologies may be crucial for health and safety of persons, the protection of the environment and climate change and for society as a whole. It is thus appropriate that under exceptional reasons of public security or protection of life and health of natural persons, environmental protection and the protection of key industrial and infrastructural assets, market surveillance authorities could authorise the placing on the market or the putting into service of AI systems which have not undergone a conformity assessment. In duly justified situations, as provided for in this Regulation, law enforcement authorities or civil protection authorities may put a specific high-risk AI system into service without the authorisation of the market surveillance authority, provided that such authorisation is requested during or after the use without undue delay.

(131) In order to facilitate the work of the Commission and the Member States in the AI field as well as to increase the transparency towards the public, providers of high-risk AI systems other than those related to products falling within the scope of relevant existing Union harmonisation legislation, as well as providers who consider that an AI system listed in the high-risk use cases in an annex to this Regulation is not high-risk on the basis of a derogation, should be required to register themselves and information about their AI system in an EU database, to be established and managed by the Commission. Before using an AI system listed in the high-risk use cases in an annex to this Regulation, deployers of high-risk AI systems that are public authorities, agencies or bodies, should register themselves in such database and select the system that they envisage to use. Other deployers should be entitled to do so voluntarily. This section of the EU database should be publicly accessible, free of charge, the information should be easily navigable, understandable and machine-readable. The EU database should also be user-friendly, for example by providing search functionalities, including through keywords, allowing the general public to find relevant information to be submitted upon the registration of high-risk AI systems and on the use case of high-risk AI systems, set out in an annex to this Regulation, to which the high-risk AI systems correspond. Any substantial modification of high-risk AI systems should also be registered in the EU database. For high-risk AI systems in the area of law enforcement, migration, asylum and border control management, the registration obligations should be fulfilled in a secure non-public section of the EU database. Access to the secure non-public section should be strictly limited to the Commission as well as to market surveillance authorities with regard to their national section of that database. High-risk AI systems in the area of critical infrastructure should only be registered at national level. The Commission should be the controller of the EU database, in accordance with Regulation (EU) 2018/1725. In order to ensure the full functionality of the EU database, when deployed, the procedure for setting the database should include the development of functional specifications by the Commission and an independent audit report. The Commission should take into account cybersecurity risks when carrying out its tasks as data controller on the EU database. In order to maximise the availability and use of the EU database by the public, the EU database, including the information made available through it, should comply with requirements under the Directive (EU) 2019/882.

(132) Certain AI systems intended to interact with natural persons or to generate content may pose specific risks of impersonation or deception irrespective of whether they qualify as high-risk or not. In certain circumstances, the use of these systems should therefore be subject to specific transparency obligations without prejudice to the requirements and obligations for high-risk AI systems and subject to targeted exceptions to take into account the special need of law enforcement. In particular, natural persons should be notified that they are interacting with an AI system, unless this is obvious from the point of view of a natural person who is reasonably well-informed, observant and circumspect taking into account the circumstances and the context of use. When implementing that obligation, the characteristics of natural persons belonging to vulnerable groups due to their age or disability should be taken into account to the extent the AI system is intended to interact with those groups as well. Moreover, natural persons should be notified when they are exposed to AI systems that, by processing their biometric data, can identify or infer the emotions or intentions of those persons or assign them to specific categories. Such specific categories can relate to aspects such as sex, age, hair colour, eye colour, tattoos, personal traits, ethnic origin, personal preferences and interests. Such information and notifications should be provided in accessible formats for persons with disabilities.

(129) 高风险人工智能系统应加贴 CE 标志，以表明其符合本条例的要求，从而能够在内部市场中自由流通。对于嵌入产品中的高风险人工智能系统，应加贴实体 CE 标志，并可由数字 CE 标志予以补充。对于仅以数字方式提供的高风险人工智能系统，应使用数字 CE 标志。成员国不得对符合本条例规定要求并加贴 CE 标志的高风险人工智能系统的投放市场或投入使用设置不合理的障碍。

(130) 在某些条件下，创新技术的快速可用性可能对人员的健康和安全、环境保护和气候变化以及整个社会至关重要。因此，在公共安全或保护自然人生命和健康、环境保护以及保护关键工业和基础设施资产的特殊理由下，市场监督机构可以授权将未经合格评定的人工智能系统投放市场或投入使用。在本条例规定的有正当理由的情形下，执法机构或民事保护机构可在未经市场监督机构授权的情况下将特定的高风险人工智能系统投入使用，但须在使用期间或使用后毫不迟延地申请该授权。

(131) 为便利委员会和成员国在人工智能领域的工作以及提高对公众的透明度，除与属于相关现有欧盟协调立法范围内的产品有关的高风险人工智能系统外，其他高风险人工智能系统的提供者，以及认为本条例附件高风险用例中所列的人工智能系统基于豁免不属于高风险的提供者，应被要求在由委员会建立和管理的欧盟数据库中登记自身及其人工智能系统的信息。在使用本条例附件高风险用例中所列的人工智能系统之前，属于公共当局、机构或机关的高风险人工智能系统部署者应在该数据库中登记自身并选择其拟使用的系统。其他部署者应有权自愿进行登记。欧盟数据库的这一部分应可公开访问、免费，信息应易于浏览、理解和机器可读。欧盟数据库还应便于用户使用，例如提供搜索功能，包括通过关键词搜索，使公众能够找到高风险人工智能系统登记时提交的相关信息以及高风险人工智能系统所对应的本条例附件中规定的高风险用例的信息。高风险人工智能系统的任何实质性修改也应在欧盟数据库中登记。对于执法、移民、庇护和边境管制管理领域的高风险人工智能系统，登记义务应在欧盟数据库的安全非公开部分履行。对安全非公开部分的访问应严格限于委员会以及就其国家部分而言的市场监督机构。关键基础设施领域的高风险人工智能系统应仅在国家层面登记。委员会应依照 Regulation (EU) 2018/1725 担任欧盟数据库的控制者。为确保欧盟数据库在部署时的完整功能，数据库的设立程序应包括委员会制定功能规范和一份独立审计报告。委员会在履行其作为欧盟数据库数据控制者的任务时应考虑网络安全风险。为最大限度地提高公众对欧盟数据库的可用性和使用，欧盟数据库，包括通过其提供的信息，应符合 Directive (EU) 2019/882 的要求。

(132) 某些旨在与自然人交互或生成内容的人工智能系统可能构成特定的冒充或欺骗风险，无论其是否属于高风险。因此，在某些情况下，这些系统的使用应遵守特定的透明度义务，而不影响高风险人工智能系统的要求和义务，并应遵守有针对性的例外以考虑执法的特殊需要。特别是，应通知自然人其正在与人工智能系统交互，除非从合理知情、善于观察和谨慎的自然人的角度来看，考虑到使用的情形和背景，这一点是显而易见的。在实施该义务时，应在人工智能系统同样旨在与因年龄或残疾而属于弱势群体的自然人交互的范围内，考虑这些群体的特征。此外，当自然人接触通过处理其生物识别数据能够识别或推断其情绪或意图或将其归入特定类别的人工智能系统时，应通知这些自然人。此类特定类别可涉及性别、年龄、发色、眼睛颜色、纹身、个人特征、族裔出身、个人偏好和兴趣等方面。此类信息和通知应以残疾人可访问的格式提供。

(133) A variety of AI systems can generate large quantities of synthetic content that becomes increasingly hard for humans to distinguish from human-generated and authentic content. The wide availability and increasing capabilities of those systems have a significant impact on the integrity and trust in the information ecosystem, raising new risks of misinformation and manipulation at scale, fraud, impersonation and consumer deception. In light of those impacts, the fast technological pace and the need for new methods and techniques to trace origin of information, it is appropriate to require providers of those systems to embed technical solutions that enable marking in a machine readable format and detection that the output has been generated or manipulated by an AI system and not a human. Such techniques and methods should be sufficiently reliable, interoperable, effective and robust as far as this is technically feasible, taking into account available techniques or a combination of such techniques, such as watermarks, metadata identifications, cryptographic methods for proving provenance and authenticity of content, logging methods, fingerprints or other techniques, as may be appropriate. When implementing this obligation, providers should also take into account the specificities and the limitations of the different types of content and the relevant technological and market developments in the field, as reflected in the generally acknowledged state of the art. Such techniques and methods can be implemented at the level of the AI system or at the level of the AI model, including general-purpose AI models generating content, thereby facilitating fulfilment of this obligation by the downstream provider of the AI system. To remain proportionate, it is appropriate to envisage that this marking obligation should not cover AI systems performing primarily an assistive function for standard editing or AI systems not substantially altering the input data provided by the deployer or the semantics thereof.

(134) Further to the technical solutions employed by the providers of the AI system, deployers who use an AI system to generate or manipulate image, audio or video content that appreciably resembles existing persons, objects, places, entities or events and would falsely appear to a person to be authentic or truthful (deep fakes), should also clearly and distinguishably disclose that the content has been artificially created or manipulated by labelling the AI output accordingly and disclosing its artificial origin. Compliance with this transparency obligation should not be interpreted as indicating that the use of the AI system or its output impedes the right to freedom of expression and the right to freedom of the arts and sciences guaranteed in the Charter, in particular where the content is part of an evidently creative, satirical, artistic, fictional or analogous work or programme, subject to appropriate safeguards for the rights and freedoms of third parties. In those cases, the transparency obligation for deep fakes set out in this Regulation is limited to disclosure of the existence of such generated or manipulated content in an appropriate manner that does not hamper the display or enjoyment of the work, including its normal exploitation and use, while maintaining the utility and quality of the work. In addition, it is also appropriate to envisage a similar disclosure obligation in relation to AI-generated or manipulated text to the extent it is published with the purpose of informing the public on matters of public interest unless the AI-generated content has undergone a process of human review or editorial control and a natural or legal person holds editorial responsibility for the publication of the content.

(135) Without prejudice to the mandatory nature and full applicability of the transparency obligations, the Commission may also encourage and facilitate the drawing up of codes of practice at Union level to facilitate the effective implementation of the obligations regarding the detection and labelling of artificially generated or manipulated content, including to support practical arrangements for making, as appropriate, the detection mechanisms accessible and facilitating cooperation with other actors along the value chain, disseminating content or checking its authenticity and provenance to enable the public to effectively distinguish AI-generated content.

(136) The obligations placed on providers and deployers of certain AI systems in this Regulation to enable the detection and disclosure that the outputs of those systems are artificially generated or manipulated are particularly relevant to facilitate the effective implementation of Regulation (EU) 2022/2065. This applies in particular as regards the obligations of providers of very large online platforms or very large online search engines to identify and mitigate systemic risks that may arise from the dissemination of content that has been artificially generated or manipulated, in particular the risk of the actual or foreseeable negative effects on democratic processes, civic discourse and electoral processes, including through disinformation. The requirement to label content generated by AI systems under this Regulation is without prejudice to the obligation in Article 16(6) of Regulation (EU) 2022/2065 for providers of hosting services to process notices on illegal content received pursuant to Article 16(1) of that Regulation and should not influence the assessment and the decision on the illegality of the specific content. That assessment should be performed solely with reference to the rules governing the legality of the content.

(133) 各种人工智能系统可以生成大量合成内容，人类越来越难以将其与人类生成的真实内容区分开来。这些系统的广泛可用性和不断增强的能力对信息生态系统的完整性和信任产生重大影响，带来了大规模虚假信息和操纵、欺诈、冒充和消费者欺骗的新风险。鉴于这些影响、技术的快速步伐以及追踪信息来源的新方法和新技术的需要，宜要求这些系统的提供者嵌入技术解决方案，使其能够以机器可读格式进行标记，并检测输出是由人工智能系统而非人类生成或操纵的。此类技术和方法应在技术可行的范围内足够可靠、可互操作、有效和稳健，同时考虑到可用的技术或此类技术的组合，例如水印、元数据标识、用于证明内容来源和真实性的密码学方法、日志记录方法、指纹或其他适当的技术。在实施该义务时，提供者还应考虑不同类型内容的特殊性和局限性以及该领域相关的技术和市场发展，如公认的最新技术水平所反映的那样。此类技术和方法可以在人工智能系统层面或人工智能模型层面实施，包括生成内容的通用人工智能模型，从而便利人工智能系统的下游提供者履行该义务。为保持相称性，宜设想该标记义务不应涵盖主要执行标准编辑辅助功能的人工智能系统或未实质性改变部署者提供的输入数据或其语义的人工智能系统。

(134) 除了人工智能系统提供者所采用的技术解决方案之外，使用人工智能系统生成或操纵在可感知程度上类似现有人员、物体、地点、实体或事件的图像、音频或视频内容，且该内容会使他人误以为其真实可信(深度伪造)的部署者，也应当通过相应标注人工智能输出并披露其人工来源的方式，清晰且可区分地披露该内容系人工创建或操纵。遵守该透明度义务不应被解释为表明使用人工智能系统或其输出妨碍了《宪章》所保障的言论自由权以及艺术与科学自由权，尤其是在该内容属于明显具有创造性、讽刺性、艺术性、虚构性或类似性质的作品或节目的一部分时，但须对第三方的权利和自由采取适当保障措施。在此类情形下，本条例规定的针对深度伪造的透明度义务仅限于以不妨碍作品展示或欣赏(包括其正常利用和使用)的适当方式披露此类生成或操纵内容的存在，同时保持作品的效用和质量。此外，对于人工智能生成或操纵的文本，在其以告知公众公共关切实事为目的而发布的情况下，也宜设想类似的披露义务，除非该人工智能生成内容已经过人工审查或编辑控制程序，且自然人或法人对该内容的发布承担编辑责任。

(135) 在不影响透明度义务的强制性和完全适用性的前提下，委员会还可以鼓励和促进在联盟层面制定行为准则，以促进有关检测和标注人工生成或操纵内容的义务的有效实施，包括支持在适当情况下使检测机制可获取的实用安排，并促进与价值链上其他参与者的合作、传播内容或核验其真实性和来源，以使公众能够有效区分人工智能生成内容。

(136) 本条例对某些人工智能系统的提供者和部署者施加的、使其能够检测和披露这些系统的输出系人工生成或操纵的义务，对于促进(EU) 2022/2065号条例的有效实施尤为相关。这尤其适用于超大型在线平台或超大型在线搜索引擎的提供者识别和缓解因传播人工生成或操纵内容而可能产生的系统性风险的义务，特别是对民主进程、公民话语和选举进程造成实际或可预见的负面影响的危险，包括通过虚假信息造成的此类影响。本条例下对人工智能系统生成内容进行标注的要求不影响(EU) 2022/2065号条例第16(6)条规定的托管服务提供者处理依据该条例第16(1)条收到的关于非法内容通知的义务，且不应影响对特定内容非法性的评估和决定。该评估应仅参照规范内容合法性的规则进行。

(137) Compliance with the transparency obligations for the AI systems covered by this Regulation should not be interpreted as indicating that the use of the AI system or its output is lawful under this Regulation or other Union and Member State law and should be without prejudice to other transparency obligations for deployers of AI systems laid down in Union or national law.

(138) AI is a rapidly developing family of technologies that requires regulatory oversight and a safe and controlled space for experimentation, while ensuring responsible innovation and integration of appropriate safeguards and risk mitigation measures. To ensure a legal framework that promotes innovation, is future-proof and resilient to disruption, Member States should ensure that their national competent authorities establish at least one AI regulatory sandbox at national level to facilitate the development and testing of innovative AI systems under strict regulatory oversight before these systems are placed on the market or otherwise put into service. Member States could also fulfil this obligation through participating in already existing regulatory sandboxes or establishing jointly a sandbox with one or more Member States' competent authorities, insofar as this participation provides equivalent level of national coverage for the participating Member States. AI regulatory sandboxes could be established in physical, digital or hybrid form and may accommodate physical as well as digital products. Establishing authorities should also ensure that the AI regulatory sandboxes have the adequate resources for their functioning, including financial and human resources.

(139) The objectives of the AI regulatory sandboxes should be to foster AI innovation by establishing a controlled experimentation and testing environment in the development and pre-marketing phase with a view to ensuring compliance of the innovative AI systems with this Regulation and other relevant Union and national law. Moreover, the AI regulatory sandboxes should aim to enhance legal certainty for innovators and the competent authorities' oversight and understanding of the opportunities, emerging risks and the impacts of AI use, to facilitate regulatory learning for authorities and undertakings, including with a view to future adaptions of the legal framework, to support cooperation and the sharing of best practices with the authorities involved in the AI regulatory sandbox, and to accelerate access to markets, including by removing barriers for SMEs, including start-ups. AI regulatory sandboxes should be widely available throughout the Union, and particular attention should be given to their accessibility for SMEs, including start-ups. The participation in the AI regulatory sandbox should focus on issues that raise legal uncertainty for providers and prospective providers to innovate, experiment with AI in the Union and contribute to evidence-based regulatory learning. The supervision of the AI systems in the AI regulatory sandbox should therefore cover their development, training, testing and validation before the systems are placed on the market or put into service, as well as the notion and occurrence of substantial modification that may require a new conformity assessment procedure. Any significant risks identified during the development and testing of such AI systems should result in adequate mitigation and, failing that, in the suspension of the development and testing process. Where appropriate, national competent authorities establishing AI regulatory sandboxes should cooperate with other relevant authorities, including those supervising the protection of fundamental rights, and could allow for the involvement of other actors within the AI ecosystem such as national or European standardisation organisations, notified bodies, testing and experimentation facilities, research and experimentation labs, European Digital Innovation Hubs and relevant stakeholder and civil society organisations. To ensure uniform implementation across the Union and economies of scale, it is appropriate to establish common rules for the AI regulatory sandboxes' implementation and a framework for cooperation between the relevant authorities involved in the supervision of the sandboxes. AI regulatory sandboxes established under this Regulation should be without prejudice to other law allowing for the establishment of other sandboxes aiming to ensure compliance with law other than this Regulation. Where appropriate, relevant competent authorities in charge of those other regulatory sandboxes should consider the benefits of using those sandboxes also for the purpose of ensuring compliance of AI systems with this Regulation. Upon agreement between the national competent authorities and the participants in the AI regulatory sandbox, testing in real world conditions may also be operated and supervised in the framework of the AI regulatory sandbox.

(140) This Regulation should provide the legal basis for the providers and prospective providers in the AI regulatory sandbox to use personal data collected for other purposes for developing certain AI systems in the public interest within the AI regulatory sandbox, only under specified conditions, in accordance with Article 6(4) and Article 9(2), point (g), of Regulation (EU) 2016/679, and Articles 5, 6 and 10 of Regulation (EU) 2018/1725, and without prejudice to Article 4(2) and Article 10 of Directive (EU) 2016/680. All other obligations of data controllers and rights of data subjects under Regulations (EU) 2016/679 and (EU) 2018/1725 and Directive (EU) 2016/680 remain applicable. In particular, this Regulation should not provide a legal basis in the meaning of Article 22(2), point (b) of Regulation (EU) 2016/679 and Article 24(2), point (b) of Regulation (EU) 2018/1725. Providers and prospective

(137) 遵守本条例所涵盖的人工智能系统的透明度义务，不应被解释为表明该人工智能系统的使用或其输出根据本条例或其他欧盟和成员国法律是合法的，并且不应影响欧盟或国家法律为人工智能系统部署者规定的其他透明度义务。

(138) 人工智能是一个快速发展的技术族群，需要监管监督以及安全和受控的试验空间，同时确保负责任的创新并纳入适当的保障措施和风险缓解措施。为确保建立一个促进创新、面向未来且具有抗干扰能力的法律框架，成员国应确保其国家主管机关在国家层面至少建立一个AI监管沙盒，以便在这些创新人工智能系统投放市场或以其他方式投入使用之前，在严格的监管监督下促进其开发和测试。成员国也可以通过参与已有的监管沙盒，或与一个或多个成员国的国家主管机关联合建立一个沙盒来履行该义务，只要此种参与为参与成员国提供同等水平的国家覆盖范围。AI监管沙盒可以实体、数字或混合形式建立，并可容纳实体产品和数字产品。建立沙盒的主管机关还应确保AI监管沙盒拥有运作所需的充足资源，包括财政和人力资源。

(139) AI监管沙盒的目标应是通过在开发和上市前阶段建立受控的试验和测试环境来促进AI创新，以确保创新人工智能系统符合本条例及其他相关联盟法和国家法。此外，AI监管沙盒应旨在增强创新者的法律确定性，并增强国家主管机关对AI利用的机会、新兴风险和影响的监督和理解，促进主管机关和企业的监管学习，包括着眼于法律框架的未来调整，支持与参与AI监管沙盒的主管机关之间的合作和最佳实践分享，并加速市场准入，包括消除中小企业(含初创企业)面临的障碍。AI监管沙盒应在整个联盟范围内广泛可用，并应特别关注中小企业(含初创企业)的可获取性。参与AI监管沙盒应侧重于为提供者和潜在提供者在联盟内创新、试验AI并促进基于证据的监管学习而带来法律不确定性的问题。因此，对AI监管沙盒中人工智能系统的监督应涵盖这些系统在投放市场或投入使用之前的开发、训练、测试和验证，以及可能需要新的合格评定程序的实质性修改的概念和发生情况。在此类人工智能系统的开发和测试期间发现的任何重大风险应导致适当的缓解措施，若无法缓解，则应暂停开发和测试过程。在适当情况下，建立AI监管沙盒的国家主管机关应与其他相关主管机关合作，包括监督基本权利保护的主管机关，并可允许AI生态系统内的其他参与者参与，例如国家或欧洲标准化组织、公告机构、测试和试验设施、研究和实验实验室、欧洲数字创新中心以及相关利益相关方和民间社会组织。为确保整个联盟的统一实施和规模经济，宜为AI监管沙盒的实施制定共同规则，并为参与沙盒监督的相关主管机关之间的合作建立框架。根据本条例建立的AI监管沙盒不应影响允许建立其他沙盒以确保遵守本条例以外法律的其他法律。在适当情况下，负责这些其他监管沙盒的相关主管机关应考虑将这些沙盒也用于确保人工智能系统符合本条例的目的所带来的益处。经国家主管机关与AI监管沙盒参与者达成一致，真实世界条件下的测试也可以在AI监管沙盒框架内运行和监督。

(140) 本条例应当为人工智能监管沙盒中的提供者和潜在提供者提供法律依据，使其能够在人工智能监管沙盒内，仅为公共利益开发特定人工智能系统的目的，使用为其他目的收集的个人数据，但须符合特定条件，并依照Regulation (EU) 2016/679第6(4)条和第9(2)条(g)点、Regulation (EU) 2018/1725第5条、第6条和第10条，且不影响Directive (EU) 2016/680第4(2)条和第10条。数据控制者在Regulation (EU) 2016/679和(EU) 2018/1725以及Directive (EU) 2016/680下的所有其他义务和数据主体的权利仍然适用。特别是，本条例不应当提供Regulation (EU) 2016/679第22(2)条(b)点和Regulation (EU) 2018/1725第24(2)条(b)点意义上的法律依据。提供者和潜在

providers in the AI regulatory sandbox should ensure appropriate safeguards and cooperate with the competent authorities, including by following their guidance and acting expeditiously and in good faith to adequately mitigate any identified significant risks to safety, health, and fundamental rights that may arise during the development, testing and experimentation in that sandbox.

(141) In order to accelerate the process of development and the placing on the market of the high-risk AI systems listed in an annex to this Regulation, it is important that providers or prospective providers of such systems may also benefit from a specific regime for testing those systems in real world conditions, without participating in an AI regulatory sandbox. However, in such cases, taking into account the possible consequences of such testing on individuals, it should be ensured that appropriate and sufficient guarantees and conditions are introduced by this Regulation for providers or prospective providers. Such guarantees should include, inter alia, requesting informed consent of natural persons to participate in testing in real world conditions, with the exception of law enforcement where the seeking of informed consent would prevent the AI system from being tested. Consent of subjects to participate in such testing under this Regulation is distinct from, and without prejudice to, consent of data subjects for the processing of their personal data under the relevant data protection law. It is also important to minimise the risks and enable oversight by competent authorities and therefore require prospective providers to have a real-world testing plan submitted to competent market surveillance authority, register the testing in dedicated sections in the EU database subject to some limited exceptions, set limitations on the period for which the testing can be done and require additional safeguards for persons belonging to certain vulnerable groups, as well as a written agreement defining the roles and responsibilities of prospective providers and deployers and effective oversight by competent personnel involved in the real world testing. Furthermore, it is appropriate to envisage additional safeguards to ensure that the predictions, recommendations or decisions of the AI system can be effectively reversed and disregarded and that personal data is protected and is deleted when the subjects have withdrawn their consent to participate in the testing without prejudice to their rights as data subjects under the Union data protection law. As regards transfer of data, it is also appropriate to envisage that data collected and processed for the purpose of testing in real-world conditions should be transferred to third countries only where appropriate and applicable safeguards under Union law are implemented, in particular in accordance with bases for transfer of personal data under Union law on data protection, while for non-personal data appropriate safeguards are put in place in accordance with Union law, such as Regulations (EU) 2022/868 ([42]) and (EU) 2023/2854 ([43]) of the European Parliament and of the Council.

(142) To ensure that AI leads to socially and environmentally beneficial outcomes, Member States are encouraged to support and promote research and development of AI solutions in support of socially and environmentally beneficial outcomes, such as AI-based solutions to increase accessibility for persons with disabilities, tackle socio-economic inequalities, or meet environmental targets, by allocating sufficient resources, including public and Union funding, and, where appropriate and provided that the eligibility and selection criteria are fulfilled, considering in particular projects which pursue such objectives. Such projects should be based on the principle of interdisciplinary cooperation between AI developers, experts on inequality and non-discrimination, accessibility, consumer, environmental, and digital rights, as well as academics.

(143) In order to promote and protect innovation, it is important that the interests of SMEs, including start-ups, that are providers or deployers of AI systems are taken into particular account. To that end, Member States should develop initiatives, which are targeted at those operators, including on awareness raising and information communication. Member States should provide SMEs, including start-ups, that have a registered office or a branch in the Union, with priority access to the AI regulatory sandboxes provided that they fulfil the eligibility conditions and selection criteria and without precluding other providers and prospective providers to access the sandboxes provided the same conditions and criteria are fulfilled. Member States should utilise existing channels and where appropriate, establish new dedicated channels for communication with SMEs, including start-ups, deployers, other innovators and, as appropriate, local public authorities, to support SMEs throughout their development path by providing guidance and responding to queries about the implementation of this Regulation. Where appropriate, these channels should work together to create synergies and ensure homogeneity in their guidance to SMEs, including start-ups, and deployers. Additionally, Member States should facilitate the participation of SMEs and other relevant stakeholders in the standardisation development processes. Moreover, the specific interests and needs of providers that are SMEs,

([42]) Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (OJ L 152, 3.6.2022, p. 1).

([43]) Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (OJ L, 2023/2854, 22.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2854/oj).

人工智能监管沙盒中的提供者应确保适当的保障措施并与主管机关合作，包括遵循其指导，迅速、诚信地采取行动，以充分缓解在该沙盒的开发、测试和实验过程中可能出现的任何已识别的对安全、健康和基本权利的重大风险。

(141) 为了加速本条例附件中所列高风险人工智能系统的开发过程和投放市场，重要的是，此类系统的提供者或潜在提供者也可以受益于在真实世界条件下测试这些系统的特定制度，而无需参与人工智能监管沙盒。然而，在此类情况下，考虑到此类测试对个人可能产生的后果，应当确保本条例为提供者或潜在提供者引入适当且充分的保障和条件。此类保障应当包括，除其他外，请求自然人同意参与真实世界条件下的测试，但执法除外，因为在执法中寻求知情同意将妨碍人工智能系统接受测试。主体根据本条例参与此类测试的同意，不同于且不影响数据主体根据相关数据保护法律对其个人数据处理所作的同意。同样重要的是，尽量减少风险并使主管机构能够进行监督，因此要求潜在提供者制定真实世界测试计划并提交给主管市场监督机构，在EU数据库的专门栏目中登记该测试(除某些有限例外外)，对测试可进行的期限设定限制，并要求对属于某些弱势群体的人员提供额外保障，以及订立书面协议，界定潜在提供者和部署者的角色和责任，并由参与真实世界测试的主管人员进行有效监督。此外，适宜设想额外保障，以确保人工智能系统的预测、建议或决定能够被有效逆转和忽略，并确保个人数据受到保护，且在主体撤回参与测试的同意时被删除，而不影响其根据联盟数据保护法律作为数据主体的权利。关于数据传输，还适宜设想，为真实世界条件下测试目的而收集和处理的数据，仅应在联盟法律下适当且可适用的保障措施得到实施时传输至第三国，特别是依照联盟数据保护法律下个人数据传输的依据，而对于非个人数据，则依照联盟法律(如欧洲议会和理事会Regulation (EU) 2022/868(42)和(EU) 2023/2854(43))实施适当保障措施。

(142) 为确保人工智能带来对社会和环境有益的结果，鼓励成员国支持和促进人工智能解决方案的研究与开发，以支持对社会和环境有益的结果，例如基于人工智能的解决方案，以增加残疾人的无障碍性、解决社会经济不平等或实现环境目标，为此分配充足资源，包括公共和联盟资金，并在适当情况下且在满足资格和选择标准的前提下，特别考虑追求此类目标的项目。此类项目应当基于人工智能开发者、不平等和非歧视、无障碍、消费者、环境和数字权利方面的专家以及学者之间的跨学科合作原则。

(143) 为了促进和保护创新，重要的是特别考虑作为人工智能系统提供者或部署者的SME(包括初创企业)的利益。为此，成员国应当制定针对这些运营者的举措，包括提高认识和信息传播。成员国应当为在联盟设有注册办事处或分支机构的SME(包括初创企业)提供优先进入人工智能监管沙盒的机会，前提是它们满足资格条件和选择标准，并且不排除其他提供者和潜在提供者在满足相同条件和标准的情况下进入沙盒。成员国应当利用现有渠道，并在适当情况下建立新的专门渠道，与SME(包括初创企业)、部署者、其他创新者以及酌情与地方公共当局沟通，通过提供指导和答复关于本条例实施的询问，支持SME的整个发展路径。在适当情况下，这些渠道应当协同工作以创造协同效应，并确保其对SME(包括初创企业)和部署者的指导具有同质性。此外，成员国应当促进SME和其他相关利益相关者参与标准化制定过程。此外，作为SME的提供者的特定利益和需求，

(42) 欧洲议会和理事会2022年5月30日关于欧洲数据治理的第(EU) 2022/868号条例及修订第(EU) 2018/1724号条例(《数据治理法》)(OJ L 152, 3.6.2022， 第1页)。

(43) 欧洲议会和理事会2023年12月13日关于公平统一规则的(欧盟)2023/2854号条例修订第(EU) 2017/2394号条例和第(EU) 2020/1828号指令(《数据法》)(OJ L, 2023/2854, 22.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2854/oj)。

including start-ups, should be taken into account when notified bodies set conformity assessment fees. The Commission should regularly assess the certification and compliance costs for SMEs, including start-ups, through transparent consultations and should work with Member States to lower such costs. For example, translation costs related to mandatory documentation and communication with authorities may constitute a significant cost for providers and other operators, in particular those of a smaller scale. Member States should possibly ensure that one of the languages determined and accepted by them for relevant providers' documentation and for communication with operators is one which is broadly understood by the largest possible number of cross-border deployers. In order to address the specific needs of SMEs, including start-ups, the Commission should provide standardised templates for the areas covered by this Regulation, upon request of the Board. Additionally, the Commission should complement Member States' efforts by providing a single information platform with easy-to-use information with regards to this Regulation for all providers and deployers, by organising appropriate communication campaigns to raise awareness about the obligations arising from this Regulation, and by evaluating and promoting the convergence of best practices in public procurement procedures in relation to AI systems. Medium-sized enterprises which until recently qualified as small enterprises within the meaning of the Annex to Commission Recommendation 2003/361/EC ([44]) should have access to those support measures, as those new medium-sized enterprises may sometimes lack the legal resources and training necessary to ensure proper understanding of, and compliance with, this Regulation.

(144) In order to promote and protect innovation, the AI-on-demand platform, all relevant Union funding programmes and projects, such as Digital Europe Programme, Horizon Europe, implemented by the Commission and the Member States at Union or national level should, as appropriate, contribute to the achievement of the objectives of this Regulation.

(145) In order to minimise the risks to implementation resulting from lack of knowledge and expertise in the market as well as to facilitate compliance of providers, in particular SMEs, including start-ups, and notified bodies with their obligations under this Regulation, the AI-on-demand platform, the European Digital Innovation Hubs and the testing and experimentation facilities established by the Commission and the Member States at Union or national level should contribute to the implementation of this Regulation. Within their respective mission and fields of competence, the AI-on-demand platform, the European Digital Innovation Hubs and the testing and experimentation Facilities are able to provide in particular technical and scientific support to providers and notified bodies.

(146) Moreover, in light of the very small size of some operators and in order to ensure proportionality regarding costs of innovation, it is appropriate to allow microenterprises to fulfil one of the most costly obligations, namely to establish a quality management system, in a simplified manner which would reduce the administrative burden and the costs for those enterprises without affecting the level of protection and the need for compliance with the requirements for high-risk AI systems. The Commission should develop guidelines to specify the elements of the quality management system to be fulfilled in this simplified manner by microenterprises.

(147) It is appropriate that the Commission facilitates, to the extent possible, access to testing and experimentation facilities to bodies, groups or laboratories established or accredited pursuant to any relevant Union harmonisation legislation and which fulfil tasks in the context of conformity assessment of products or devices covered by that Union harmonisation legislation. This is, in particular, the case as regards expert panels, expert laboratories and reference laboratories in the field of medical devices pursuant to Regulations (EU) 2017/745 and (EU) 2017/746.

(148) This Regulation should establish a governance framework that both allows to coordinate and support the application of this Regulation at national level, as well as build capabilities at Union level and integrate stakeholders in the field of AI. The effective implementation and enforcement of this Regulation require a governance framework that allows to coordinate and build up central expertise at Union level. The AI Office was established by Commission Decision ([45]) and has as its mission to develop Union expertise and capabilities in the field of AI and to contribute to the implementation of Union law on AI. Member States should facilitate the tasks of the AI Office with a view to support the development of Union expertise and capabilities at Union level and to strengthen the functioning of the digital single market. Furthermore, a Board composed of representatives of the Member States, a scientific panel to integrate the scientific community and an advisory forum to contribute stakeholder input to the implementation of this Regulation, at Union and national level, should be established. The development of Union expertise and

([44]) Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

([45]) Commission Decision of 24.1.2024 establishing the European Artificial Intelligence Office C(2024) 390.

包括初创企业，应当在公告机构设定合格评定费用时予以考虑。委员会应当通过透明磋商定期评估SME(包括初创企业)的认证和合规成本，并应当与成员国合作降低此类成本。例如，与强制性文件编制和与主管机构沟通相关的翻译成本可能对提供者和其他运营者，特别是规模较小的运营者构成重大成本。成员国应当尽可能确保，其确定并接受的用于相关提供者文件编制和与运营者沟通的语言之一，是尽可能多的跨境部署者广泛理解的语言。为了满足SME(包括初创企业)的特定需求，委员会应当应委员会的请求，为本条例所涵盖的领域提供标准化模板。此外，委员会应当补充成员国的努力，为所有提供者和部署者提供一个单一信息平台，提供关于本条例的易于使用的信息，组织适当的宣传运动以提高对本条例所产生义务的认识，并评估和促进人工智能系统相关公共采购程序中最佳实践的趋同。直到最近仍符合Commission Recommendation 2003/361/EC(44)附件意义上小型企业资格的中型企业应当能够获得这些支持措施，因为这些新的中型企业有时可能缺乏确保正确理解和遵守本条例所需的法律资源和培训。

(144) 为促进和保护创新，人工智能按需平台、所有相关欧盟资助计划和项目，如由委员会和成员国在欧盟或国家层面实施的“数字欧洲计划”、“地平线欧洲”，应酌情为实现本条例的目标作出贡献。

(145) 为尽量减少因市场缺乏知识和专业知识而导致的实施风险，以及为便利提供者，特别是包括初创企业在内的中小企业，和公告机构遵守本条例规定的义务，委员会和成员国在联盟或国家层面建立的人工智能按需平台、欧洲数字创新中心以及测试和实验设施应当为本条例的实施作出贡献。在各自的任务和职权范围内，人工智能按需平台、欧洲数字创新中心以及测试和实验设施能够特别为提供者和公告机构提供技术和科学支持。

(146) 此外，鉴于某些运营者的规模非常小，并为了确保创新成本方面的相称性，宜允许微型企业以简化方式履行最昂贵的义务之一，即建立质量管理体系，从而减轻这些企业的行政负担和成本，同时不影响保护水平以及遵守高风险人工智能系统要求的必要性。委员会应当制定指南，明确微型企业以这种简化方式应当履行的质量管理体系要素。

(147) 委员会宜尽可能促进各机构、团体或实验室获取测试和实验设施，这些机构、团体或实验室系依据任何相关欧盟协调立法设立或认可，并履行该欧盟协调立法所涵盖产品或设备合格评定范围内的任务。尤其是依据第(EU) 2017/745号和第(EU) 2017/746号条例在医疗器械领域的专家组、专家实验室和参考实验室。

(148) 本条例应当建立一个治理框架，既能够协调和支持本条例在国家层面的适用，又能够在联盟层面建设能力并将人工智能领域的利益相关方纳入其中。本条例的有效实施和执行需要一个能够协调并在联盟层面建立核心专业知识的治理框架。人工智能办公室由委员会决定(45)设立，其使命是发展联盟在人工智能领域的专业知识和能力，并促进联盟人工智能法律的实施。成员国应当为人工智能办公室的任务提供便利，以支持在联盟层面发展联盟专业知识和能力，并加强数字单一市场的运作。此外，应当设立一个由成员国代表组成的委员会、一个整合科学界的科学小组以及一个为联盟和国家层面本条例的实施提供利益相关方意见的咨询论坛。发展联盟专业知识和

(44) 2003年5月6日委员会关于微型、小型和中型企业定义的建议(OJ L 124, 20.5.2003 ，第36页)

(45) 委员会2024年1月24日设立欧洲人工智能办公室的决定C(2024) 390。

capabilities should also include making use of existing resources and expertise, in particular through synergies with structures built up in the context of the Union level enforcement of other law and synergies with related initiatives at Union level, such as the EuroHPC Joint Undertaking and the AI testing and experimentation facilities under the Digital Europe Programme.

(149) In order to facilitate a smooth, effective and harmonised implementation of this Regulation a Board should be established. The Board should reflect the various interests of the AI eco-system and be composed of representatives of the Member States. The Board should be responsible for a number of advisory tasks, including issuing opinions, recommendations, advice or contributing to guidance on matters related to the implementation of this Regulation, including on enforcement matters, technical specifications or existing standards regarding the requirements established in this Regulation and providing advice to the Commission and the Member States and their national competent authorities on specific questions related to AI. In order to give some flexibility to Member States in the designation of their representatives in the Board, such representatives may be any persons belonging to public entities who should have the relevant competences and powers to facilitate coordination at national level and contribute to the achievement of the Board's tasks. The Board should establish two standing sub-groups to provide a platform for cooperation and exchange among market surveillance authorities and notifying authorities on issues related, respectively, to market surveillance and notified bodies. The standing subgroup for market surveillance should act as the administrative cooperation group (ADCO) for this Regulation within the meaning of Article 30 of Regulation (EU) 2019/1020. In accordance with Article 33 of that Regulation, the Commission should support the activities of the standing subgroup for market surveillance by undertaking market evaluations or studies, in particular with a view to identifying aspects of this Regulation requiring specific and urgent coordination among market surveillance authorities. The Board may establish other standing or temporary sub-groups as appropriate for the purpose of examining specific issues. The Board should also cooperate, as appropriate, with relevant Union bodies, experts groups and networks active in the context of relevant Union law, including in particular those active under relevant Union law on data, digital products and services.

(150) With a view to ensuring the involvement of stakeholders in the implementation and application of this Regulation, an advisory forum should be established to advise and provide technical expertise to the Board and the Commission. To ensure a varied and balanced stakeholder representation between commercial and non-commercial interest and, within the category of commercial interests, with regards to SMEs and other undertakings, the advisory forum should comprise inter alia industry, start-ups, SMEs, academia, civil society, including the social partners, as well as the Fundamental Rights Agency, ENISA, the European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC) and the European Telecommunications Standards Institute (ETSI).

(151) To support the implementation and enforcement of this Regulation, in particular the monitoring activities of the AI Office as regards general-purpose AI models, a scientific panel of independent experts should be established. The independent experts constituting the scientific panel should be selected on the basis of up-to-date scientific or technical expertise in the field of AI and should perform their tasks with impartiality, objectivity and ensure the confidentiality of information and data obtained in carrying out their tasks and activities. To allow the reinforcement of national capacities necessary for the effective enforcement of this Regulation, Member States should be able to request support from the pool of experts constituting the scientific panel for their enforcement activities.

(152) In order to support adequate enforcement as regards AI systems and reinforce the capacities of the Member States, Union AI testing support structures should be established and made available to the Member States.

(153) Member States hold a key role in the application and enforcement of this Regulation. In that respect, each Member State should designate at least one notifying authority and at least one market surveillance authority as national competent authorities for the purpose of supervising the application and implementation of this Regulation. Member States may decide to appoint any kind of public entity to perform the tasks of the national competent authorities within the meaning of this Regulation, in accordance with their specific national organisational characteristics and needs. In order to increase organisation efficiency on the side of Member States and to set a single point of contact vis-à-vis the public and other counterparts at Member State and Union levels, each Member State should designate a market surveillance authority to act as a single point of contact.

能力还应包括利用现有资源和专业知识，特别是通过与欧盟层面执行其他法律所建立的结构产生协同效应，以及与欧盟层面相关倡议产生协同效应，如EuroHPC联合执行体和"数字欧洲计划"下的人工智能测试和实验设施。

(149) 为了促进本条例顺利、有效和协调地实施，应当设立一个委员会。该委员会应当反映人工智能生态系统的各种利益，并由成员国代表组成。该委员会应当负责若干咨询任务，包括就与本条例实施相关的事项发表意见、建议、咨询或协助制定指导意见，包括关于执法事项、技术规范或与本条例所确立要求相关的现有标准，并就与人工智能相关的具体问题向委员会、成员国及其国家主管机关提供建议。为了给成员国在指定其委员会代表方面提供一定灵活性，此类代表可以是属于公共实体的任何人员，其应当具备相关权限和权力，以促进国家层面的协调并协助实现委员会的任务。该委员会应当设立两个常设分组，分别为市场监督机构和公告机构就与市场监督和公告机构相关的问题提供合作与交流平台。市场监督常设分组应当作为本条例意义上欧洲议会和理事会条例(EU) 2019/1020第30条所指的行政合作组(ADCO)行事。根据该条例第33条，委员会应当通过开展市场评估或研究来支持市场监督常设分组的活动，特别是为了确定本条例中需要市场监督机构之间进行具体和紧急协调的方面。该委员会可以视情况设立其他常设或临时分组，以审查具体问题。该委员会还应当酌情与在相关联盟法律背景下活跃的相关联盟机构、专家组和网络合作，特别是与在相关联盟数据、数字产品和服务法律下活跃的机构合作。

(150) 为了确保利益相关方参与本条例的实施和适用，应当设立一个咨询论坛，向委员会和欧盟委员会提供建议和技术专业知识。为确保商业利益与非商业利益之间以及商业利益类别内部在中小企业和其他企业方面具有多样和平衡的利益相关方代表性，咨询论坛应当包括业界、初创企业、中小企业、学术界、公民社会(包括社会伙伴)以及基本权利机构、ENISA、欧洲标准化委员会(CEN)、欧洲电工标准化委员会(CENELEC)和欧洲电信标准化协会(ETSI)。

(151) 为支持本条例的实施和执法，特别是人工智能办公室对通用人工智能模型的监测活动，应设立一个由独立专家组成的科学小组。组成科学小组的独立专家应根据人工智能领域最新的科学或技术专业知识遴选，并应公正、客观地履行其任务，确保在开展任务和活动过程中所获得的信息和数据的保密性。为加强有效执行本条例所必需的国家能力，成员国应能够请求由科学小组组成的专家库为其执法活动提供支持。

(152) 为支持对人工智能系统的充分执法并加强成员国的能力，应建立欧盟人工智能测试支持结构并向成员国提供。

(153) 成员国在适用和执行本条例方面发挥关键作用。在这方面，每个成员国应指定至少一个通知机构和至少一个市场监督机构作为国家主管机关，以监督本条例的适用和实施。成员国可根据其特定的国家组织特点和需要，决定任命任何类型的公共实体履行本条例所指国家主管机关的任务。为提高成员国方面的组织效率，并在成员国和欧盟层面设立面向公众和其他对应方的单一联络点，每个成员国应指定一个市场监督机构作为单一联络点。

(154) The national competent authorities should exercise their powers independently, impartially and without bias, so as to safeguard the principles of objectivity of their activities and tasks and to ensure the application and implementation of this Regulation. The members of these authorities should refrain from any action incompatible with their duties and should be subject to confidentiality rules under this Regulation.

(155) In order to ensure that providers of high-risk AI systems can take into account the experience on the use of high-risk AI systems for improving their systems and the design and development process or can take any possible corrective action in a timely manner, all providers should have a post-market monitoring system in place. Where relevant, post-market monitoring should include an analysis of the interaction with other AI systems including other devices and software. Post-market monitoring should not cover sensitive operational data of deployers which are law enforcement authorities. This system is also key to ensure that the possible risks emerging from AI systems which continue to 'learn' after being placed on the market or put into service can be more efficiently and timely addressed. In this context, providers should also be required to have a system in place to report to the relevant authorities any serious incidents resulting from the use of their AI systems, meaning incident or malfunctioning leading to death or serious damage to health, serious and irreversible disruption of the management and operation of critical infrastructure, infringements of obligations under Union law intended to protect fundamental rights or serious damage to property or the environment.

(156) In order to ensure an appropriate and effective enforcement of the requirements and obligations set out by this Regulation, which is Union harmonisation legislation, the system of market surveillance and compliance of products established by Regulation (EU) 2019/1020 should apply in its entirety. Market surveillance authorities designated pursuant to this Regulation should have all enforcement powers laid down in this Regulation and in Regulation (EU) 2019/1020 and should exercise their powers and carry out their duties independently, impartially and without bias. Although the majority of AI systems are not subject to specific requirements and obligations under this Regulation, market surveillance authorities may take measures in relation to all AI systems when they present a risk in accordance with this Regulation. Due to the specific nature of Union institutions, agencies and bodies falling within the scope of this Regulation, it is appropriate to designate the European Data Protection Supervisor as a competent market surveillance authority for them. This should be without prejudice to the designation of national competent authorities by the Member States. Market surveillance activities should not affect the ability of the supervised entities to carry out their tasks independently, when such independence is required by Union law.

(157) This Regulation is without prejudice to the competences, tasks, powers and independence of relevant national public authorities or bodies which supervise the application of Union law protecting fundamental rights, including equality bodies and data protection authorities. Where necessary for their mandate, those national public authorities or bodies should also have access to any documentation created under this Regulation. A specific safeguard procedure should be set for ensuring adequate and timely enforcement against AI systems presenting a risk to health, safety and fundamental rights. The procedure for such AI systems presenting a risk should be applied to high-risk AI systems presenting a risk, prohibited systems which have been placed on the market, put into service or used in violation of the prohibited practices laid down in this Regulation and AI systems which have been made available in violation of the transparency requirements laid down in this Regulation and present a risk.

(158) Union financial services law includes internal governance and risk-management rules and requirements which are applicable to regulated financial institutions in the course of provision of those services, including when they make use of AI systems. In order to ensure coherent application and enforcement of the obligations under this Regulation and relevant rules and requirements of the Union financial services legal acts, the competent authorities for the supervision and enforcement of those legal acts, in particular competent authorities as defined in Regulation (EU) No 575/2013 of the European Parliament and of the Council ([46]) and Directives 2008/48/EC ([47]), 2009/138/EC ([48]),

([46]) Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1).

([47]) Directive 2008/48/EC of the European Parliament and of the Council of 23 April 2008 on credit agreements for consumers and repealing Council Directive 87/102/EEC (OJ L 133, 22.5.2008, p. 66).

([48]) Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II) (OJ L 335, 17.12.2009, p. 1).

(154) 国家主管机关应独立、公正、无偏见地行使其权力，以保障其活动和任务的客观性原则，并确保本条例的适用和实施。这些机关的成员应避免任何与其职责不符的行为，并应遵守本条例规定的保密规则。

(155) 为确保高风险人工智能系统的提供者能够考虑使用高风险人工智能系统的经验以改进其系统及设计和开发过程，或能够及时采取任何可能的纠正措施，所有提供者均应建立上市后监测系统。在相关情况下，上市后监测应包括对与其他人工智能系统(包括其他设备和软件)交互的分析。上市后监测不应涵盖作为执法机构的部署者的敏感操作数据。该系统对于确保能够更有效和及时地应对人工智能系统在投放市场或投入使用后继续"学习"所产生的可能风险也至关重要。在此背景下，还应要求提供者建立系统，向相关主管机关报告因使用其人工智能系统而产生的任何严重事件，即导致死亡或严重健康损害、关键基础设施管理和运行严重且不可逆中断、违反旨在保护基本权利的欧盟法律义务或对财产或环境造成严重损害的事件或故障。

(156) 为确保适当和有效地执行本条例(属欧盟协调立法)所规定的要求和义务，由Regulation (EU) 2019/1020建立的市场监督和产品合规体系应整体适用。根据本条例指定的市场监督机构应拥有本条例和Regulation (EU) 2019/1020规定的全部执法权力，并应独立、公正和无偏见地行使权力和履行职责。尽管大多数人工智能系统不受本条例特定要求和义务的约束，但市场监督机构可在所有人工智能系统根据本条例构成风险时对其采取措施。鉴于属于本条例适用范围的欧盟机构、机关和团体的特殊性质，宜指定欧洲数据保护监督员为其主管市场监督机构。这不应影响成员国对国家主管机关的指定。当欧盟法律要求独立性时，市场监督活动不应影响受监督实体独立履行其任务的能力。

(157) 本条例不影响监督旨在保护基本权利的欧盟法律适用的相关国家公共主管机关或机构的职权、任务、权力和独立性，包括平等机构和数据保护机构。在其职责必要时，这些国家公共主管机关或机构也应能够获取根据本条例创建的任何文件。应设定具体的保障程序，以确保对构成健康、安全和基本权利风险的人工智能系统进行充分和及时的执法。针对此类构成风险的人工智能系统的程序应适用于构成风险的高风险人工智能系统、违反本条例规定的禁止性实践而投放市场、投入使用或使用的被禁止系统，以及违反本条例规定的透明度要求而提供并构成风险的人工智能系统。

(158) 欧盟金融服务法律包含内部治理和风险管理规则与要求，这些规则与要求适用于受监管金融机构在提供此类服务过程中，包括在其使用人工智能系统时。为确保本法规项下义务与欧盟金融服务法律法案相关规则和要求的一致适用与执行，对这些法律法案进行监督和执行的主管机构，特别是欧洲议会和理事会第(EU) No 575/2013号法规(46)以及第2008/48/EC号指令(47)、第2009/138/EC号指令(48)、

(46) 欧洲议会和理事会2013年6月26日关于信贷机构和投资公司审慎要求的第(EU) No 575/2013号条例及修订第(EU) No 648/2012号条例(OJ L 176, 27.6.2013， 第1页)。

(47) 欧洲议会和理事会2008年4月23日关于消费者信贷协议的第2008/48/EC号指令及废止理事会第87/102/EEC号指令(OJ L 133, 22.5.2008, p.66)。欧洲议会和理事会2009年11月25日关于从事和经营保险与再保险业务(偿付能力II)(OJ L 335, 17.12.2009, p.1)的第2009/138/EC号指令。

2013/36/EU ([49]), 2014/17/EU ([50]) and (EU) 2016/97 ([51]) of the European Parliament and of the Council, should be designated, within their respective competences, as competent authorities for the purpose of supervising the implementation of this Regulation, including for market surveillance activities, as regards AI systems provided or used by regulated and supervised financial institutions unless Member States decide to designate another authority to fulfil these market surveillance tasks. Those competent authorities should have all powers under this Regulation and Regulation (EU) 2019/1020 to enforce the requirements and obligations of this Regulation, including powers to carry our *ex post* market surveillance activities that can be integrated, as appropriate, into their existing supervisory mechanisms and procedures under the relevant Union financial services law. It is appropriate to envisage that, when acting as market surveillance authorities under this Regulation, the national authorities responsible for the supervision of credit institutions regulated under Directive 2013/36/EU, which are participating in the Single Supervisory Mechanism established by Council Regulation (EU) No 1024/2013 ([52]), should report, without delay, to the European Central Bank any information identified in the course of their market surveillance activities that may be of potential interest for the European Central Bank's prudential supervisory tasks as specified in that Regulation. To further enhance the consistency between this Regulation and the rules applicable to credit institutions regulated under Directive 2013/36/EU, it is also appropriate to integrate some of the providers' procedural obligations in relation to risk management, post marketing monitoring and documentation into the existing obligations and procedures under Directive 2013/36/EU. In order to avoid overlaps, limited derogations should also be envisaged in relation to the quality management system of providers and the monitoring obligation placed on deployers of high-risk AI systems to the extent that these apply to credit institutions regulated by Directive 2013/36/EU. The same regime should apply to insurance and re-insurance undertakings and insurance holding companies under Directive 2009/138/EC and the insurance intermediaries under Directive (EU) 2016/97 and other types of financial institutions subject to requirements regarding internal governance, arrangements or processes established pursuant to the relevant Union financial services law to ensure consistency and equal treatment in the financial sector.

(159) Each market surveillance authority for high-risk AI systems in the area of biometrics, as listed in an annex to this Regulation insofar as those systems are used for the purposes of law enforcement, migration, asylum and border control management, or the administration of justice and democratic processes, should have effective investigative and corrective powers, including at least the power to obtain access to all personal data that are being processed and to all information necessary for the performance of its tasks. The market surveillance authorities should be able to exercise their powers by acting with complete independence. Any limitations of their access to sensitive operational data under this Regulation should be without prejudice to the powers conferred to them by Directive (EU) 2016/680. No exclusion on disclosing data to national data protection authorities under this Regulation should affect the current or future powers of those authorities beyond the scope of this Regulation.

(160) The market surveillance authorities and the Commission should be able to propose joint activities, including joint investigations, to be conducted by market surveillance authorities or market surveillance authorities jointly with the Commission, that have the aim of promoting compliance, identifying non-compliance, raising awareness and providing guidance in relation to this Regulation with respect to specific categories of high-risk AI systems that are found to present a serious risk across two or more Member States. Joint activities to promote compliance should be carried out in accordance with Article 9 of Regulation (EU) 2019/1020. The AI Office should provide coordination support for joint investigations.

(161) It is necessary to clarify the responsibilities and competences at Union and national level as regards AI systems that are built on general-purpose AI models. To avoid overlapping competences, where an AI system is based on a general-purpose AI model and the model and system are provided by the same provider, the supervision should

([49]) Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (OJ L 176, 27.6.2013, p. 338).

([50]) Directive 2014/17/EU of the European Parliament and of the Council of 4 February 2014 on credit agreements for consumers relating to residential immovable property and amending Directives 2008/48/EC and 2013/36/EU and Regulation (EU) No 1093/2010 (OJ L 60, 28.2.2014, p. 34).

([51]) Directive (EU) 2016/97 of the European Parliament and of the Council of 20 January 2016 on insurance distribution (OJ L 26, 2.2.2016, p. 19).

([52]) Council Regulation (EU) No 1024/2013 of 15 October 2013 conferring specific tasks on the European Central Bank concerning policies relating to the prudential supervision of credit institutions (OJ L 287, 29.10.2013, p. 63).

欧洲议会和理事会第2013/36/EU号指令（49）、第2014/17/EU号指令（50）和第（EU）2016/97号指令（51）应在各自职权范围内被指定为本条例实施监督的主管机构，包括就受监管和监督的金融机构所提供或使用的人工智能系统开展市场监督活动，除非成员国决定指定另一机构履行这些市场监督任务。这些主管机构应拥有本条例和第（EU）2019/1020号条例规定的所有权力，以执行本条例的要求和义务，包括开展可酌情纳入相关欧盟金融服务法下现有监督机制和程序的事后市场监督活动的权力。宜设想，在作为本条例下的市场监督机构行事时，负责监督受第2013/36/EU号指令监管且参与根据理事会第（EU）No 1024/2013号条例（52）建立的单一监督机制的信贷机构的各国主管机构，应毫不迟延地向欧洲中央银行报告其市场监督活动中发现的、可能对欧洲中央银行根据该条例规定的审慎监督任务具有潜在利益的任何信息。为进一步增强本条例与适用于受第2013/36/EU号指令监管的信贷机构的规则之间的一致性，还宜将提供者在风险管理、上市后监测和文件方面的部分程序性义务纳入第2013/36/EU号指令下的现有义务和程序。为避免重叠，还宜设想在提供者的质量管理体系以及赋予高风险人工智能系统部署者的监测义务方面作出有限减损，前提是这些义务适用于受第2013/36/EU号指令监管的信贷机构。同一制度应适用于第2009/138/EC号指令下的保险和再保险企业及保险控股公司、第（EU）2016/97号指令下的保险中介机构以及受依据相关欧盟金融服务法确立的内部治理、安排或程序要求约束的其他类型金融机构，以确保金融部门的一致性和平等待遇。

(159) 本法规附件所列生物识别领域高风险人工智能系统的各市场监督机构，在這些系统用于执法、移民、庇护和边境管制管理或司法和民主进程管理的目的时，应当拥有有效的调查和纠正权力，至少包括获取正在处理的所有个人数据以及履行职责所需的所有信息的权力。市场监督机构应当能够完全独立地行使权力。本法规对其获取敏感业务数据的任何限制不应影响第(EU) 2016/680号指令赋予其的权力。本法规关于向国家数据保护机构披露数据的任何排除，不应影响这些机构在本法规范围之外的当前或未来权力。

(160) 市场监督机构和委员会应能够提出联合活动，包括联合

由市场监督机构或市场监督机构与委员会联合开展的调查，旨在促进合规、识别不合规、提高认识并针对本法规就发现在两个或更多成员国构成严重风险的特定类别高风险人工智能系统提供指导。促进合规的联合活动应当根据第(EU) 2019/1020号法规第9条开展。人工智能办公室应当为联合调查提供协调支持。

(161) 有必要明确欧盟和国家层面对基于通用人工智能模型的人工智能系统的职责和权限。

为避免权限重叠，当人工智能系统基于通用人工智能模型且该模型和系统由同一提供者提供时，监督应

(49) 欧洲议会和理事会2013年6月26日关于信贷机构业务准入及信贷机构和投资公司审慎监管的第2013/36/EU号指令，修订第2002/87/EC号指令并废止第2006/48/EC号和第2006/49/EC号指令(OJ L 176, 27.6.2013， 第338页)。

(50) 欧洲议会和理事会2014年2月4日关于住宅不动产消费者信贷协议的第2014/17/EU号指令及修订第2008/48/EC号和第2013/36/EU号指令及第(EU) No 1093/2010号条例(OJ L 60, 28.2.2014， 第34页)。

(51) 欧洲议会和理事会2016年1月20日关于保险分销的指令(EU) 2016/97(OJ L 26, 2.2.2016 ，第

(52) 19 页) 。

理事会2013年10月15日关于授予欧洲中央银行涉及信贷机构审慎监管政策特定任务的第(EU) No 1024/2013号条例(OJ L 287, 29.10.2013， 第63页)。

take place at Union level through the AI Office, which should have the powers of a market surveillance authority within the meaning of Regulation (EU) 2019/1020 for this purpose. In all other cases, national market surveillance authorities remain responsible for the supervision of AI systems. However, for general-purpose AI systems that can be used directly by deployers for at least one purpose that is classified as high-risk, market surveillance authorities should cooperate with the AI Office to carry out evaluations of compliance and inform the Board and other market surveillance authorities accordingly. Furthermore, market surveillance authorities should be able to request assistance from the AI Office where the market surveillance authority is unable to conclude an investigation on a high-risk AI system because of its inability to access certain information related to the general-purpose AI model on which the high-risk AI system is built. In such cases, the procedure regarding mutual assistance in cross-border cases in Chapter VI of Regulation (EU) 2019/1020 should apply *mutatis mutandis*.

(162) To make best use of the centralised Union expertise and synergies at Union level, the powers of supervision and enforcement of the obligations on providers of general-purpose AI models should be a competence of the Commission. The AI Office should be able to carry out all necessary actions to monitor the effective implementation of this Regulation as regards general-purpose AI models. It should be able to investigate possible infringements of the rules on providers of general-purpose AI models both on its own initiative, following the results of its monitoring activities, or upon request from market surveillance authorities in line with the conditions set out in this Regulation. To support effective monitoring of the AI Office, it should provide for the possibility that downstream providers lodge complaints about possible infringements of the rules on providers of general-purpose AI models and systems.

(163) With a view to complementing the governance systems for general-purpose AI models, the scientific panel should support the monitoring activities of the AI Office and may, in certain cases, provide qualified alerts to the AI Office which trigger follow-ups, such as investigations. This should be the case where the scientific panel has reason to suspect that a general-purpose AI model poses a concrete and identifiable risk at Union level. Furthermore, this should be the case where the scientific panel has reason to suspect that a general-purpose AI model meets the criteria that would lead to a classification as general-purpose AI model with systemic risk. To equip the scientific panel with the information necessary for the performance of those tasks, there should be a mechanism whereby the scientific panel can request the Commission to require documentation or information from a provider.

(164) The AI Office should be able to take the necessary actions to monitor the effective implementation of and compliance with the obligations for providers of general-purpose AI models laid down in this Regulation. The AI Office should be able to investigate possible infringements in accordance with the powers provided for in this Regulation, including by requesting documentation and information, by conducting evaluations, as well as by requesting measures from providers of general-purpose AI models. When conducting evaluations, in order to make use of independent expertise, the AI Office should be able to involve independent experts to carry out the evaluations on its behalf. Compliance with the obligations should be enforceable, inter alia, through requests to take appropriate measures, including risk mitigation measures in the case of identified systemic risks as well as restricting the making available on the market, withdrawing or recalling the model. As a safeguard, where needed beyond the procedural rights provided for in this Regulation, providers of general-purpose AI models should have the procedural rights provided for in Article 18 of Regulation (EU) 2019/1020, which should apply *mutatis mutandis*, without prejudice to more specific procedural rights provided for by this Regulation.

(165) The development of AI systems other than high-risk AI systems in accordance with the requirements of this Regulation may lead to a larger uptake of ethical and trustworthy AI in the Union. Providers of AI systems that are not high-risk should be encouraged to create codes of conduct, including related governance mechanisms, intended to foster the voluntary application of some or all of the mandatory requirements applicable to high-risk AI systems, adapted in light of the intended purpose of the systems and the lower risk involved and taking into account the available technical solutions and industry best practices such as model and data cards. Providers and, as appropriate, deployers of all AI systems, high-risk or not, and AI models should also be encouraged to apply on a voluntary basis additional requirements related, for example, to the elements of the Union's Ethics Guidelines for Trustworthy AI,

在欧盟层面通过人工智能办公室进行，为此目的，人工智能办公室应当拥有第(EU) 2019/1020号法规含义范围内的市场监督机构权力。在所有其他情况下，国家市场监督机构仍负责对人工智能系统的监督。然而，对于部署者可直接用于至少一种被归类为高风险的用途的通用人工智能系统，市场监督机构应当与人工智能办公室合作开展合规评估，并相应通知委员会和其他市场监督机构。此外，在市场监督机构因无法获取与高风险人工智能系统所基于的通用人工智能模型相关的某些信息而无法完成对高风险人工智能系统的调查时，市场监督机构应当能够请求人工智能办公室提供协助。在此类情况下，第(EU) 2019/1020号法规第六章关于跨境案件互助的程序应当比照适用。

(162) 为最佳利用集中化的联盟专业知识和联盟层面的协同效应，对通用人工智能模型提供者义务的监督和执行权力应属于委员会的职权。人工智能办公室应能够采取一切必要行动，监督本条例关于通用人工智能模型的有效实施。它应能够主动地、根据其监测活动的结果，或应市场监督机构依照本条例规定的条件提出的请求，调查通用人工智能模型提供者可能违反规则的行为。为支持人工智能办公室的有效监测，应规定下游提供者可就通用人工智能模型和系统提供者可能违反规则的行为提出投诉的可能性。

(163) 为补充通用人工智能模型的治理体系，科学小组应支持人工智能办公室的监测活动，并可在某些情况下向人工智能办公室提供触发后续行动(如调查)的合格警报。在科学小组有理由怀疑某通用人工智能模型在联盟层面构成具体且可识别的风险的情况下，应如此。此外，在科学小组有理由怀疑某通用人工智能模型符合将被归类为具有系统性风险的通用人工智能模型的标准的情况下，也应如此。为使科学小组具备履行这些任务所需的信息，应建立一种机制，使科学小组能够请求委员会要求提供者提供文件或信息。

(164) 人工智能办公室应能够采取必要行动，监督本条例规定的通用人工智能模型提供者义务的有效实施和遵守情况。人工智能办公室应能够依照本条例规定的权力调查可能的违规行为，包括通过要求提供文件和信息、开展评估以及要求通用人工智能模型提供者采取措施。在开展评估时，为利用独立专业知识，人工智能办公室应能够聘请独立专家代表其开展评估。对义务的遵守应可强制执行，除其他外，可通过要求采取适当措施，包括在已识别系统性风险的情况下采取风险缓解措施，以及限制模型投放市场、撤回或召回模型。作为一项保障，在本条例规定的程序性权利之外有需要时，通用人工智能模型提供者应享有Regulation(EU) 2019/1020第18条规定的程序性权利，该权利应*mutatis mutandis*适用，不影响本条例规定的更具体的程序性权利。

(165) 按照本条例要求开发高风险人工智能系统以外的人工智能系统，可能会促进伦理和可信人工智能在联盟内更广泛的采用。应鼓励非高风险人工智能系统的提供者制定行为准则，包括相关治理机制，旨在促进自愿适用适用于高风险人工智能系统的部分或全部强制性要求，并根据系统的预期目的和所涉较低风险进行调整，同时考虑可用的技术解决方案和行业最佳实践，如模型卡和数据卡。还应鼓励所有人工智能系统(无论是否高风险)和人工智能模型的提供者以及酌情包括部署者，自愿适用附加要求，例如与联盟《可信人工智能伦理准则》的要素相关的要求，

environmental sustainability, AI literacy measures, inclusive and diverse design and development of AI systems, including attention to vulnerable persons and accessibility to persons with disability, stakeholders' participation with the involvement, as appropriate, of relevant stakeholders such as business and civil society organisations, academia, research organisations, trade unions and consumer protection organisations in the design and development of AI systems, and diversity of the development teams, including gender balance. To ensure that the voluntary codes of conduct are effective, they should be based on clear objectives and key performance indicators to measure the achievement of those objectives. They should also be developed in an inclusive way, as appropriate, with the involvement of relevant stakeholders such as business and civil society organisations, academia, research organisations, trade unions and consumer protection organisation. The Commission may develop initiatives, including of a sectoral nature, to facilitate the lowering of technical barriers hindering cross-border exchange of data for AI development, including on data access infrastructure, semantic and technical interoperability of different types of data.

(166) It is important that AI systems related to products that are not high-risk in accordance with this Regulation and thus are not required to comply with the requirements set out for high-risk AI systems are nevertheless safe when placed on the market or put into service. To contribute to this objective, Regulation (EU) 2023/988 of the European Parliament and of the Council ([53]) would apply as a safety net.

(167) In order to ensure trustful and constructive cooperation of competent authorities on Union and national level, all parties involved in the application of this Regulation should respect the confidentiality of information and data obtained in carrying out their tasks, in accordance with Union or national law. They should carry out their tasks and activities in such a manner as to protect, in particular, intellectual property rights, confidential business information and trade secrets, the effective implementation of this Regulation, public and national security interests, the integrity of criminal and administrative proceedings, and the integrity of classified information.

(168) Compliance with this Regulation should be enforceable by means of the imposition of penalties and other enforcement measures. Member States should take all necessary measures to ensure that the provisions of this Regulation are implemented, including by laying down effective, proportionate and dissuasive penalties for their infringement, and to respect the *ne bis in idem* principle. In order to strengthen and harmonise administrative penalties for infringement of this Regulation, the upper limits for setting the administrative fines for certain specific infringements should be laid down. When assessing the amount of the fines, Member States should, in each individual case, take into account all relevant circumstances of the specific situation, with due regard in particular to the nature, gravity and duration of the infringement and of its consequences and to the size of the provider, in particular if the provider is an SME, including a start-up. The European Data Protection Supervisor should have the power to impose fines on Union institutions, agencies and bodies falling within the scope of this Regulation.

(169) Compliance with the obligations on providers of general-purpose AI models imposed under this Regulation should be enforceable, inter alia, by means of fines. To that end, appropriate levels of fines should also be laid down for infringement of those obligations, including the failure to comply with measures requested by the Commission in accordance with this Regulation, subject to appropriate limitation periods in accordance with the principle of proportionality. All decisions taken by the Commission under this Regulation are subject to review by the Court of Justice of the European Union in accordance with the TFEU, including the unlimited jurisdiction of the Court of Justice with regard to penalties pursuant to Article 261 TFEU.

(170) Union and national law already provide effective remedies to natural and legal persons whose rights and freedoms are adversely affected by the use of AI systems. Without prejudice to those remedies, any natural or legal person that has grounds to consider that there has been an infringement of this Regulation should be entitled to lodge a complaint to the relevant market surveillance authority.

(171) Affected persons should have the right to obtain an explanation where a deployer's decision is based mainly upon the output from certain high-risk AI systems that fall within the scope of this Regulation and where that decision produces legal effects or similarly significantly affects those persons in a way that they consider to have an adverse

([53]) Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC (OJ L 135, 23.5.2023, p. 1).

环境可持续性、人工智能素养措施、人工智能系统的包容性和多样性设计与开发(包括关注弱势群体和残疾人的无障碍性)、利益相关者的参与(酌情让企业和民间社会组织、学术界、研究机构、工会和消费者保护组织等相关利益相关者参与人工智能系统的设计与开发)以及开发团队的多样性(包括性别平衡)。为确保自愿行为准则的有效性，其应基于明确的目标和衡量这些目标实现情况的关键绩效指标。其还应酌情以包容的方式制定，让企业和民间社会组织、学术界、研究机构、工会和消费者保护组织等相关利益相关者参与。委员会可制定举措，包括部门性举措，以促进降低阻碍人工智能开发数据跨境交换的技术壁垒，包括在数据访问基础设施、不同类型数据的语义和技术互操作性方面。

(166) 重要的是，根据本条例不属于高风险因而无需遵守高风险人工智能系统所规定要求的相关产品的人工智能系统，在投放市场或投入使用时应仍然安全。为促进这一目标，欧洲议会和理事会第(EU) 2023/988号条例(53)将作为安全网适用。

(167) 为确保联盟和国家层面主管当局之间值得信赖和建设性的合作，参与本法规适用的各方应依照联盟或国家法律，对在履行职责过程中获取的信息和数据保密。它们应以保护知识产权、保密商业信息和商业秘密、本法规的有效实施、公共和国家利益、刑事和行政诉讼的完整性以及机密信息的完整性等方式履行职责和开展活动。

(168) 对本法规的遵守应通过处以罚款和其他执法措施予以强制执行。成员国应采取一切必要措施确保本法规的规定得到实施，包括对违反本法规的行为规定有效、相称和具有威慑力的罚款，并遵守一事不再罚原则。为加强和统一对违反本法规行为的行政处罚，应规定对某些特定违法行为设定行政罚款的上限。在评估罚款金额时，成员国应在每个具体案件中考虑具体情况的所有相关情节，尤其应适当考虑违法行为的性质、严重程度和持续时间及其后果，以及提供者的规模，特别是当提供者属于中小企业(包括初创企业)时。欧洲数据保护监督机构应有权对属于本法规适用范围的联盟机构、机关和团体处以罚款。

(169) 对通用人工智能模型提供者依本法规承担的义务的遵守，应通过包括罚款在内的方式予以强制执行。为此，还应针对违反这些义务的行为规定适当水平的罚款，包括未能遵守委员会依本法规要求采取的措施，但须符合依照相称性原则规定的适当时效期限。委员会依本法规作出的所有决定均须依照TFEU接受欧盟法院的审查，包括欧盟法院依照TFEU第261条对处罚享有的无限管辖权。

(170) 欧盟和国家法律已为权利和自由因人工智能系统的使用而受到不利影响的自然人和法人提供了有效救济。在不影响这些救济的情况下，任何有理由认为存在违反本条例行为的自然人或法人应有权向相关市场监督机构提出投诉。

(171) 受影响者应有权在部署者的决定主要基于属于本条例适用范围某些高风险人工智能系统的输出，且该决定产生法律效力或类似地显著影响这些人，使其认为受到不利影响时，获得解释。

(53) 欧洲议会和理事会2023年5月10日关于一般产品安全的(EU) 2023/988号条例，修订
欧洲议会和理事会第(EU) No 1025/2012号条例和欧洲议会和理事会第(EU) 2020/1828号指令，并废止欧洲议会和理事会第2001/95/EC号指令和理事会第87/357/EEC号指令(OJ L 135, 23.5.2023， 第1页)。

impact on their health, safety or fundamental rights. That explanation should be clear and meaningful and should provide a basis on which the affected persons are able to exercise their rights. The right to obtain an explanation should not apply to the use of AI systems for which exceptions or restrictions follow from Union or national law and should apply only to the extent this right is not already provided for under Union law.

(172) Persons acting as whistleblowers on the infringements of this Regulation should be protected under the Union law. Directive (EU) 2019/1937 of the European Parliament and of the Council ([54]) should therefore apply to the reporting of infringements of this Regulation and the protection of persons reporting such infringements.

(173) In order to ensure that the regulatory framework can be adapted where necessary, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission to amend the conditions under which an AI system is not to be considered to be high-risk, the list of high-risk AI systems, the provisions regarding technical documentation, the content of the EU declaration of conformity the provisions regarding the conformity assessment procedures, the provisions establishing the high-risk AI systems to which the conformity assessment procedure based on assessment of the quality management system and assessment of the technical documentation should apply, the threshold, benchmarks and indicators, including by supplementing those benchmarks and indicators, in the rules for the classification of general-purpose AI models with systemic risk, the criteria for the designation of general-purpose AI models with systemic risk, the technical documentation for providers of general-purpose AI models and the transparency information for providers of general-purpose AI models. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making ([55]). In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

(174) Given the rapid technological developments and the technical expertise required to effectively apply this Regulation, the Commission should evaluate and review this Regulation by 2 August 2029 and every four years thereafter and report to the European Parliament and the Council. In addition, taking into account the implications for the scope of this Regulation, the Commission should carry out an assessment of the need to amend the list of high-risk AI systems and the list of prohibited practices once a year. Moreover, by 2 August 2028 and every four years thereafter, the Commission should evaluate and report to the European Parliament and to the Council on the need to amend the list of high-risk areas headings in the annex to this Regulation, the AI systems within the scope of the transparency obligations, the effectiveness of the supervision and governance system and the progress on the development of standardisation deliverables on energy efficient development of general-purpose AI models, including the need for further measures or actions. Finally, by 2 August 2028 and every three years thereafter, the Commission should evaluate the impact and effectiveness of voluntary codes of conduct to foster the application of the requirements provided for high-risk AI systems in the case of AI systems other than high-risk AI systems and possibly other additional requirements for such AI systems.

(175) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council ([56]).

(176) Since the objective of this Regulation, namely to improve the functioning of the internal market and to promote the uptake of human centric and trustworthy AI, while ensuring a high level of protection of health, safety, fundamental rights enshrined in the Charter, including democracy, the rule of law and environmental protection against harmful effects of AI systems in the Union and supporting innovation, cannot be sufficiently achieved by the Member States and can rather, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt

([54]) Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law (OJ L 305, 26.11.2019, p. 17).
([55]) OJ L 123, 12.5.2016, p. 1.
([56]) Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

对其健康、安全或基本权利的影响。该解释应当清晰且有意义，并应为受影响者行使自身权利提供依据。获得解释的权利不应适用于因欧盟或国家法律而产生例外或限制的人工智能系统使用情形，且仅在本条例未在欧盟法律下已规定该权利的情况下适用。

(172) 就违反本条例行为进行举报的举报人应受到欧盟法律保护。

因此，欧洲议会和理事会 Directive (EU) 2019/1937(54) 应适用于对本条例违反行为的举报以及对举报此类违反行为者的保护。

(173) 为确保监管框架在必要时能够调整，应授权委员会根据TFEU第290条通过法案，以修订人工智能系统不被视为高风险的条件、高风险人工智能系统清单、关于技术文档的规定、欧盟符合性声明的内容、关于合格评定程序的规定、确立应适用基于质量管理体系评估和技术文档评估的合格评定程序的高风险人工智能系统的规定、具有系统性风险的通用人工智能模型分类规则中的阈值、基准和指标(包括补充这些基准和指标)、具有系统性风险的通用人工智能模型的指定标准、通用人工智能模型提供者的技术文档以及通用人工智能模型提供者的透明度信息。委员会在其准备工作中进行适当磋商(包括专家层面的磋商)尤为重要，且这些磋商应按照2016年4月13日《关于改进立法的机构间协议》(55)所规定的原则进行。特别是，为确保平等参与授权法案的准备工作，欧洲议会和理事会应与成员国专家同时收到所有文件，且其专家应系统性地有权参加委员会处理授权法案准备工作的专家小组会议。

(174) 鉴于技术快速发展以及有效适用本条例所需的技术专长，委员会应于2029年8月2日之前及此后每四年对本条例进行评估和审查，并向欧洲议会和理事会报告。此外，考虑到对本条例适用范围的影响，委员会应每年对是否有必要修订高风险人工智能系统清单和禁止性实践清单进行评估。并且，委员会应于2028年8月2日之前及此后每四年，就以下事项进行评估并向欧洲议会和理事会报告：是否有必要修订本条例附件中的高风险领域标题清单、属于透明度义务范围内的人工智能系统、监督与治理体系的有效性，以及关于通用人工智能模型能效开发的标准化交付成果的制定进展，包括是否需要采取进一步措施或行动。最后，委员会应于2028年8月2日之前及此后每三年，评估自愿行为准则在促进非高风险人工智能系统情形下适用高风险人工智能系统所规定要求方面的影响和有效性，以及对此类人工智能系统可能施加的其他附加要求。

(175) 为确保本条例实施的统一条件，实施权力应

授予委员会。该等权力应按照欧洲议会和理事会 Regulation (EU) No 182/2011(56) 行使。

(176) 鉴于本条例的目标，即改善内部市场的运作并促进

以人为本和可信人工智能的采用，同时确保高水平保护《宪章》所载的健康、安全、基本权利，包括民主、法治和环境保护，免受人工智能系统在欧盟内的有害影响，并支持创新，这些目标无法由成员国充分实现，而是由于行动的规模或效果，在欧盟层面能够更好地实现，因此欧盟可以采取

(54) 欧洲议会和理事会2019年10月23日关于保护举报违反联盟法行为者的指令(EU) 2019/1937(OJ L 305,2019年11月26日，第17页)。
(55) OJ L 123, 12.5.2016， 第1页。
(56) 欧洲议会和理事会 2011年2月16日规定成员国对委员会行使实施权力进行控制的机制规则和一般原则的 Regulation (EU) No 182/2011(OJ L 55, 28.2.2011, p.13)。

measures in accordance with the principle of subsidiarity as set out in Article 5 TEU. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

(177) In order to ensure legal certainty, ensure an appropriate adaptation period for operators and avoid disruption to the market, including by ensuring continuity of the use of AI systems, it is appropriate that this Regulation applies to the high-risk AI systems that have been placed on the market or put into service before the general date of application thereof, only if, from that date, those systems are subject to significant changes in their design or intended purpose. It is appropriate to clarify that, in this respect, the concept of significant change should be understood as equivalent in substance to the notion of substantial modification, which is used with regard only to high-risk AI systems pursuant to this Regulation. On an exceptional basis and in light of public accountability, operators of AI systems which are components of the large-scale IT systems established by the legal acts listed in an annex to this Regulation and operators of high-risk AI systems that are intended to be used by public authorities should, respectively, take the necessary steps to comply with the requirements of this Regulation by end of 2030 and by 2 August 2030.

(178) Providers of high-risk AI systems are encouraged to start to comply, on a voluntary basis, with the relevant obligations of this Regulation already during the transitional period.

(179) This Regulation should apply from 2 August 2026. However, taking into account the unacceptable risk associated with the use of AI in certain ways, the prohibitions as well as the general provisions of this Regulation should already apply from 2 February 2025. While the full effect of those prohibitions follows with the establishment of the governance and enforcement of this Regulation, anticipating the application of the prohibitions is important to take account of unacceptable risks and to have an effect on other procedures, such as in civil law. Moreover, the infrastructure related to the governance and the conformity assessment system should be operational before 2 August 2026, therefore the provisions on notified bodies and governance structure should apply from 2 August 2025. Given the rapid pace of technological advancements and adoption of general-purpose AI models, obligations for providers of general-purpose AI models should apply from 2 August 2025. Codes of practice should be ready by 2 May 2025 in view of enabling providers to demonstrate compliance on time. The AI Office should ensure that classification rules and procedures are up to date in light of technological developments. In addition, Member States should lay down and notify to the Commission the rules on penalties, including administrative fines, and ensure that they are properly and effectively implemented by the date of application of this Regulation. Therefore the provisions on penalties should apply from 2 August 2025.

(180) The European Data Protection Supervisor and the European Data Protection Board were consulted in accordance with Article 42(1) and (2) of Regulation (EU) 2018/1725 and delivered their joint opinion on 18 June 2021,

HAVE ADOPTED THIS REGULATION:

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter`

1. The purpose of this Regulation is to improve the functioning of the internal market and promote the uptake of human-centric and trustworthy artificial intelligence (AI), while ensuring a high level of protection of health, safety, fundamental rights enshrined in the Charter, including democracy, the rule of law and environmental protection, against the harmful effects of AI systems in the Union and supporting innovation.

2. This Regulation lays down:

(a) harmonised rules for the placing on the market, the putting into service, and the use of AI systems in the Union;

依照《欧盟条约》第5条规定的辅助性原则采取措施。依照该条规定的比例性原则，本条例不超出实现该目标所必需的范围。

(177) 为确保法律确定性、确保运营者具有适当的适应期并避免对

市场，包括通过确保人工智能系统使用的连续性，本法规适用于在其一般适用日期之前已投放市场或投入使用的高风险人工智能系统是适当的，但仅当自该日期起，这些系统的设计或预期用途发生重大变化时。有必要澄清，在这方面，重大变化的概念应理解为在实质上等同于实质性修改的概念，后者仅根据本法规针对高风险人工智能系统使用。作为例外情况并鉴于公共问责制，作为本法规附件所列法律法案建立的大规模IT系统组成部分的人工智能系统的运营者以及拟由公共当局使用的高风险人工智能系统的运营者，应分别在2030年底前和2030年8月2日前采取必要步骤遵守本法规的要求。

(178) 鼓励高风险人工智能系统的提供者在自愿基础上开始遵守相关

本 Regulation 的义务在过渡期内已经适用。

(179) 本条例应自 2 August 2026 起适用。然而，考虑到与以下相关的不可接受风险

对于以某些方式使用人工智能的情形，本法规的禁止性规定以及一般条款应自2025年2月2日起适用。尽管这些禁止性规定的完整效力有待本法规治理与执行机制的建立，但提前适用这些禁止性规定对于应对不可接受的风险并对其他程序(例如民法程序)产生影响具有重要意义。此外，与治理和合格评定制度相关的基础设施应在2026年8月2日之前投入运行，因此关于公告机构和治理结构的条款应自2025年8月2日起适用。鉴于技术进步的快速步伐和通用人工智能模型的采用，通用人工智能模型提供者的义务应自2025年8月2日起适用。行为准则应于2025年5月2日前准备就绪，以使提供者能够按时证明合规。人工智能办公室应确保分类规则和程序根据技术发展保持最新。此外，成员国应制定并向委员会通报关于处罚(包括行政罚款)的规则，并确保在本法规适用之日这些规则得到妥善有效的实施。因此，关于处罚的条款应自2025年8月2日起适用。

(180) 欧洲数据保护监督员和欧洲数据保护委员会已依照

与(EU) 2018/1725号条例第42(1)条和第(2)条，并于2021年6月18日提交了它们的联合意见，

通过本条例：

第一章

一般规定

第1条

事项`

1. 本条例的目的是改善内部市场的运作，促进以人为本且可信人工智能(AI)的采用，同时在欧盟范围内确保对健康、安全、《宪章》所载基本权利(包括民主、法治和环境保护)的高水平保护，使其免受人工智能系统有害影响，并支持创新。

2. 本法规规定：

(a) 关于在欧盟境内投放市场、投入使用和使用人工智能系统的协调规则；

(b) prohibitions of certain AI practices;

(c) specific requirements for high-risk AI systems and obligations for operators of such systems;

(d) harmonised transparency rules for certain AI systems;

(e) harmonised rules for the placing on the market of general-purpose AI models;

(f) rules on market monitoring, market surveillance, governance and enforcement;

(g) measures to support innovation, with a particular focus on SMEs, including start-ups.

Article 2

Scope

1. This Regulation applies to:

(a) providers placing on the market or putting into service AI systems or placing on the market general-purpose AI models in the Union, irrespective of whether those providers are established or located within the Union or in a third country;

(b) deployers of AI systems that have their place of establishment or are located within the Union;

(c) providers and deployers of AI systems that have their place of establishment or are located in a third country, where the output produced by the AI system is used in the Union;

(d) importers and distributors of AI systems;

(e) product manufacturers placing on the market or putting into service an AI system together with their product and under their own name or trademark;

(f) authorised representatives of providers, which are not established in the Union;

(g) affected persons that are located in the Union.

2. For AI systems classified as high-risk AI systems in accordance with Article 6(1) related to products covered by the Union harmonisation legislation listed in Section B of Annex I, only Article 6(1), Articles 102 to 109 and Article 112 apply. Article 57 applies only in so far as the requirements for high-risk AI systems under this Regulation have been integrated in that Union harmonisation legislation.

3. This Regulation does not apply to areas outside the scope of Union law, and shall not, in any event, affect the competences of the Member States concerning national security, regardless of the type of entity entrusted by the Member States with carrying out tasks in relation to those competences.

This Regulation does not apply to AI systems where and in so far they are placed on the market, put into service, or used with or without modification exclusively for military, defence or national security purposes, regardless of the type of entity carrying out those activities.

This Regulation does not apply to AI systems which are not placed on the market or put into service in the Union, where the output is used in the Union exclusively for military, defence or national security purposes, regardless of the type of entity carrying out those activities.

4. This Regulation applies neither to public authorities in a third country nor to international organisations falling within the scope of this Regulation pursuant to paragraph 1, where those authorities or organisations use AI systems in the framework of international cooperation or agreements for law enforcement and judicial cooperation with the Union or with one or more Member States, provided that such a third country or international organisation provides adequate safeguards with respect to the protection of fundamental rights and freedoms of individuals.

5. This Regulation shall not affect the application of the provisions on the liability of providers of intermediary services as set out in Chapter II of Regulation (EU) 2022/2065.

(b) 某些人工智能实践的禁令；

(c) 对高风险人工智能系统的具体要求以及此类系统运营者的义务；

(d) 针对特定人工智能系统的统一透明度规则；

(e) 通用人工智能模型投放市场的一致规则；

(f) 市场监测、市场监督、治理与执行规则；

(g) 支持创新的措施，特别侧重于中小企业，包括初创企业。

第2条

范围

1. 本条例适用于：

(a) 在欧盟境内投放市场或投入使用人工智能系统或投放市场通用人工智能模型的提供者，无论该等提供者是否设立或位于欧盟境内或第三国；

(b) 设立地或位于欧盟境内的人工智能系统部署者；

(c) 设立地或位于第三国的人工智能系统提供者和部署者，且人工智能系统产生的输出在欧盟境内使用；

(d) AI系统的进口商和分销商；

(e) 将人工智能系统与其产品一同并以自身名称或商标投放市场或投入使用产品制造商；

(f) 未在欧盟设立的提供者的授权代表；

(g) 位于欧盟境内的受影响人员。

2. 对于依照 Article 6(1) 被归类为高风险人工智能系统、且与 Annex I 的 Section B 所列欧盟协调立法所涵盖产品相关的人工智能系统，仅适用 Article 6(1)、Articles 102 to 109 和 Article 112。Article 57 仅在本条例下高风险人工智能系统的要求已纳入该欧盟协调立法的范围内适用。

3. 本条例不适用于欧盟法律范围之外的领域，并且在任何情况下均不影响成员国在国家安全方面的权限，无论成员国委托何种类型的实体执行与该等权限相关的任务。

本条例不适用于仅用于军事、国防或国家安全目的(无论是否经修改)而投放市场、投入使用或使用的人工智能系统，无论执行这些活动的实体类型如何。

本条例不适用于未在欧盟投放市场或投入使用、但其输出在欧盟仅用于军事、国防或国家安全目的的人工智能系统，无论执行这些活动的实体类型如何。

4. 本法规既不适用于第三国的公共当局，也不适用于根据第1款属于本法规适用范围的国际组织，前提是这些当局或组织在与欧盟或一个或多个成员国的执法和司法合作框架内使用人工智能系统，且该第三国或国际组织在保护个人基本权利和自由方面提供充分保障。

5. 本条例不影响 Regulation (EU) 2022/2065 第II章所规定的中间服务提供者责任条款的适用。

6. This Regulation does not apply to AI systems or AI models, including their output, specifically developed and put into service for the sole purpose of scientific research and development.

7. Union law on the protection of personal data, privacy and the confidentiality of communications applies to personal data processed in connection with the rights and obligations laid down in this Regulation. This Regulation shall not affect Regulation (EU) 2016/679 or (EU) 2018/1725, or Directive 2002/58/EC or (EU) 2016/680, without prejudice to Article 10(5) and Article 59 of this Regulation.

8. This Regulation does not apply to any research, testing or development activity regarding AI systems or AI models prior to their being placed on the market or put into service. Such activities shall be conducted in accordance with applicable Union law. Testing in real world conditions shall not be covered by that exclusion.

9. This Regulation is without prejudice to the rules laid down by other Union legal acts related to consumer protection and product safety.

10. This Regulation does not apply to obligations of deployers who are natural persons using AI systems in the course of a purely personal non-professional activity.

11. This Regulation does not preclude the Union or Member States from maintaining or introducing laws, regulations or administrative provisions which are more favourable to workers in terms of protecting their rights in respect of the use of AI systems by employers, or from encouraging or allowing the application of collective agreements which are more favourable to workers.

12. This Regulation does not apply to AI systems released under free and open-source licences, unless they are placed on the market or put into service as high-risk AI systems or as an AI system that falls under Article 5 or 50.

Article 3

Definitions

For the purposes of this Regulation, the following definitions apply:

(1) 'AI system' means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments;

(2) 'risk' means the combination of the probability of an occurrence of harm and the severity of that harm;

(3) 'provider' means a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge;

(4) 'deployer' means a natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity;

(5) 'authorised representative' means a natural or legal person located or established in the Union who has received and accepted a written mandate from a provider of an AI system or a general-purpose AI model to, respectively, perform and carry out on its behalf the obligations and procedures established by this Regulation;

(6) 'importer' means a natural or legal person located or established in the Union that places on the market an AI system that bears the name or trademark of a natural or legal person established in a third country;

(7) 'distributor' means a natural or legal person in the supply chain, other than the provider or the importer, that makes an AI system available on the Union market;

(8) 'operator' means a provider, product manufacturer, deployer, authorised representative, importer or distributor;

6. 本条例不适用于仅为科学研究与开发这一唯一目的而专门开发并投入使用的人工智能系统或人工智能模型，包括其输出。

7. 欧盟关于个人数据保护、隐私和通信保密的法律适用于与本条例所规定权利和义务相关而处理的个人数据。在不影响本条例 Article 10(5) 和 Article 59 的情况下，本条例不影响 Regulation (EU) 2016/679 或 (EU) 2018/1725，或 Directive 2002/58/EC 或 (EU) 2016/680。

8. 本条例不适用于人工智能系统或人工智能模型在投放市场或投入使用之前进行的任何研究、测试或开发活动。该等活动应按照适用的欧盟法律进行。真实世界条件下的测试不属于该排除范围。

9. 本条例不影响其他欧盟法律文件就消费者保护和产品安全所规定的规则。

10. 本条例不适用于作为自然人纯粹在个人非职业活动中使用人工智能系统的部署者的义务。

11. 本条例不阻止欧盟或成员国维持或引入在雇主使用人工智能系统方面更有利于保护劳动者权利的法律、法规或行政规定，也不阻止鼓励或允许适用更有利于劳动者的集体协议。

12. 本条例不适用于以免费和开源许可证发布的人工智能系统，除非它们作为高风险人工智能系统或属于Article 5或50范围的人工智能系统投放市场或投入使用。

第3条

定义

就本条例而言，适用以下定义：

(1) “人工智能系统”是指一种基于机器的系统，其设计为以不同程度的自主性运行，并可能在部署后表现出适应性，且其出于明确或隐含的目标，从所接收的输入中推断如何生成可影响物理或虚拟环境的输出，如预测、内容、建议或决定；

(2) “风险”是指发生损害的概率与该损害严重程度的组合；

(3) “提供者”是指开发人工智能系统或通用人工智能模型，或委托开发人工智能系统或通用人工智能模型，并以自身名义或商标将其投放市场或投入使用(无论是否收费)的自然人或法人、公共机构、机关或其他团体；

(4) “部署者”是指在其权限下使用人工智能系统的自然人或法人、公共机构、机关或其他团体，但在个人非职业活动中使用人工智能系统的除外；

(5) “授权代表”是指在欧盟境内设立或成立的、已收到并接受人工智能系统或通用人工智能模型提供者的书面授权，以代表其履行和执行本条例所规定义务和程序的自然人或法人；

(6) “进口商”是指在欧盟境内设立或成立的、将带有在第三国设立的自然人或法人名称或商标的人工智能系统投放市场的自然人或法人；

(7) “分销商”是指供应链中除提供者或进口商以外的、在欧盟市场上提供人工智能系统的自然人或法人；

(8) “运营者”是指提供者、产品制造商、部署者、授权代表、进口商或分销商；

(9) ‘placing on the market’ means the first making available of an AI system or a general-purpose AI model on the Union market;

(10) ‘making available on the market’ means the supply of an AI system or a general-purpose AI model for distribution or use on the Union market in the course of a commercial activity, whether in return for payment or free of charge;

(11) ‘putting into service’ means the supply of an AI system for first use directly to the deployer or for own use in the Union for its intended purpose;

(12) ‘intended purpose’ means the use for which an AI system is intended by the provider, including the specific context and conditions of use, as specified in the information supplied by the provider in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation;

(13) ‘reasonably foreseeable misuse’ means the use of an AI system in a way that is not in accordance with its intended purpose, but which may result from reasonably foreseeable human behaviour or interaction with other systems, including other AI systems;

(14) ‘safety component’ means a component of a product or of an AI system which fulfils a safety function for that product or AI system, or the failure or malfunctioning of which endangers the health and safety of persons or property;

(15) ‘instructions for use’ means the information provided by the provider to inform the deployer of, in particular, an AI system’s intended purpose and proper use;

(16) ‘recall of an AI system’ means any measure aiming to achieve the return to the provider or taking out of service or disabling the use of an AI system made available to deployers;

(17) ‘withdrawal of an AI system’ means any measure aiming to prevent an AI system in the supply chain being made available on the market;

(18) ‘performance of an AI system’ means the ability of an AI system to achieve its intended purpose;

(19) ‘notifying authority’ means the national authority responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring;

(20) ‘conformity assessment’ means the process of demonstrating whether the requirements set out in Chapter III, Section 2 relating to a high-risk AI system have been fulfilled;

(21) ‘conformity assessment body’ means a body that performs third-party conformity assessment activities, including testing, certification and inspection;

(22) ‘notified body’ means a conformity assessment body notified in accordance with this Regulation and other relevant Union harmonisation legislation;

(23) ‘substantial modification’ means a change to an AI system after its placing on the market or putting into service which is not foreseen or planned in the initial conformity assessment carried out by the provider and as a result of which the compliance of the AI system with the requirements set out in Chapter III, Section 2 is affected or results in a modification to the intended purpose for which the AI system has been assessed;

(24) ‘CE marking’ means a marking by which a provider indicates that an AI system is in conformity with the requirements set out in Chapter III, Section 2 and other applicable Union harmonisation legislation providing for its affixing;

(25) ‘post-market monitoring system’ means all activities carried out by providers of AI systems to collect and review experience gained from the use of AI systems they place on the market or put into service for the purpose of identifying any need to immediately apply any necessary corrective or preventive actions;

(26) ‘market surveillance authority’ means the national authority carrying out the activities and taking the measures pursuant to Regulation (EU) 2019/1020;

(9) “投放市场”是指人工智能系统或通用人工智能模型首次在欧盟市场上提供；

(10) “在市场上提供”是指在商业活动中为在欧盟市场上分销或使用而供应人工智能系统或通用人工智能模型，无论是否收费；

(11) “投入使用”是指为首次直接向部署者供应人工智能系统，或在欧盟境内为其自身预期目的使用而供应人工智能系统；

(12) “预期目的”是指提供者所预期的人工智能系统用途，包括使用说明、宣传或销售材料和声明中以及技术文档中提供者所提供信息中规定的具体使用背景和条件；

(13) “合理可预见的误用”是指以不符合其预期目的的方式使用人工智能系统，但该使用可能源于合理可预见的人类行为或与其他系统(包括其他人工智能系统)的交互；

(14) “安全组件”是指产品人工智能系统的组件，其履行该产品或人工智能系统的安全功能，或其故障或失灵危及人身健康和安全或财产安全；

(15) “使用说明”是指提供者提供的、用于告知部署者人工智能系统预期目的和正确使用方式等信息；

(16) “召回人工智能系统”是指旨在实现将已向部署者提供的人工智能系统退回提供者、停止使用或禁用其使用的任何措施；

(17) “撤回人工智能系统”是指旨在防止供应链中的人工智能系统在市场上提供的任何措施；

(18) “人工智能系统的性能”是指人工智能系统实现其预期目的的能力；

(19) “通知机构”指负责建立和开展合格评定机构评估、指定和通知及其监督必要程序的国家机构；

(20) “合格评定”是指证明高风险人工智能系统是否满足第三章第2节所规定要求的程序；

(21) “合格评定机构”是指执行第三方合格评定活动(包括测试、认证和检验)的机构；

(22) “公告机构”是指依照本条例和其他相关欧盟协调立法被通知的合格评定机构；

(23) “实质性修改”是指人工智能系统在投放市场或投入使用后发生的、提供者在初始合格评定中未预见或计划的变更，且该变更导致人工智能系统对第三章第2节所规定要求的符合性受到影响，或导致对该人工智能系统已评估的预期目的发生修改；

(24) “CE标志”是指提供者用以表明人工智能系统符合第三章第2节所规定要求以及规定加贴该标志的其他适用欧盟协调立法的标志；

(25) “上市后监测系统”是指人工智能系统提供者为收集和审查从其投放市场或投入使用的人工智能系统使用中获得的经验而开展的所有活动，目的是识别是否需要立即采取任何必要的纠正或预防措施；

(26) “市场监督机构”是指依照(EU) 2019/1020号条例开展活动并采取措施的国家机关；

(27) ‘harmonised standard’ means a harmonised standard as defined in Article 2(1), point (c), of Regulation (EU) No 1025/2012;

(28) ‘common specification’ means a set of technical specifications as defined in Article 2, point (4) of Regulation (EU) No 1025/2012, providing means to comply with certain requirements established under this Regulation;

(29) ‘training data’ means data used for training an AI system through fitting its learnable parameters;

(30) ‘validation data’ means data used for providing an evaluation of the trained AI system and for tuning its non-learnable parameters and its learning process in order, inter alia, to prevent underfitting or overfitting;

(31) ‘validation data set’ means a separate data set or part of the training data set, either as a fixed or variable split;

(32) ‘testing data’ means data used for providing an independent evaluation of the AI system in order to confirm the expected performance of that system before its placing on the market or putting into service;

(33) ‘input data’ means data provided to or directly acquired by an AI system on the basis of which the system produces an output;

(34) ‘biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, such as facial images or dactyloscopic data;

(35) ‘biometric identification’ means the automated recognition of physical, physiological, behavioural, or psychological human features for the purpose of establishing the identity of a natural person by comparing biometric data of that individual to biometric data of individuals stored in a database;

(36) ‘biometric verification’ means the automated, one-to-one verification, including authentication, of the identity of natural persons by comparing their biometric data to previously provided biometric data;

(37) ‘special categories of personal data’ means the categories of personal data referred to in Article 9(1) of Regulation (EU) 2016/679, Article 10 of Directive (EU) 2016/680 and Article 10(1) of Regulation (EU) 2018/1725;

(38) ‘sensitive operational data’ means operational data related to activities of prevention, detection, investigation or prosecution of criminal offences, the disclosure of which could jeopardise the integrity of criminal proceedings;

(39) ‘emotion recognition system’ means an AI system for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data;

(40) ‘biometric categorisation system’ means an AI system for the purpose of assigning natural persons to specific categories on the basis of their biometric data, unless it is ancillary to another commercial service and strictly necessary for objective technical reasons;

(41) ‘remote biometric identification system’ means an AI system for the purpose of identifying natural persons, without their active involvement, typically at a distance through the comparison of a person’s biometric data with the biometric data contained in a reference database;

(42) ‘real-time remote biometric identification system’ means a remote biometric identification system, whereby the capturing of biometric data, the comparison and the identification all occur without a significant delay, comprising not only instant identification, but also limited short delays in order to avoid circumvention;

(43) ‘post-remote biometric identification system’ means a remote biometric identification system other than a real-time remote biometric identification system;

(44) ‘publicly accessible space’ means any publicly or privately owned physical place accessible to an undetermined number of natural persons, regardless of whether certain conditions for access may apply, and regardless of the potential capacity restrictions;

(27) “协调标准”指(EU) No 1025/2012号条例第2(1)条第(c)点所定义的协调标准；

(28) “通用规范”指(EU) No 1025/2012号条例第2条第(4)点所定义的一套技术规范，提供遵守本条例所确立的某些要求的手段；

(29) “训练数据”指通过拟合人工智能系统的可学习参数而用于训练该系统的数据；

(30) “验证数据”指用于对已训练的人工智能系统进行评价并用于调整其不可学习参数及其学习过程的数据，目的尤其包括防止欠拟合或过拟合；

(31) “验证数据集”指单独的数据集或训练数据集的一部分，可以是固定划分或可变划分；

(32) “测试数据”指用于对人工智能系统进行独立评价以在该系统投放市场或投入使用之前确认其预期性能的数据；

(33) “输入数据”指提供给人工智能系统或由该系统直接获取的、系统据以产生输出的数据；

(34) “生物特征数据”指与自然人的身体、生理或行为特征有关的特定技术处理所产生的个人数据，例如面部图像或指纹数据；

(35) “生物特征识别”指为确定自然人身份的目的，通过将该个人的生物特征数据与数据库中存储的个人的生物特征数据进行比较，对自然人的身体、生理、行为或心理特征进行的自动化识别；

(36) “生物特征验证”指通过将自然人的生物特征数据与先前提供的生物特征数据进行比较，对自然人身份进行的自动化一对一验证，包括认证；

(37) “特殊类别的个人数据”指(EU) 2016/679号条例第9(1)条、(EU) 2016/680号指令第10条和(EU) 2018/1725号条例第10(1)条所指的个人数据类别；

(38) “敏感业务数据”指与预防、侦查、调查或起诉刑事犯罪活动有关的业务数据，其披露可能危及刑事诉讼的完整性；

(39) “情绪识别系统”指为根据自然人的生物特征数据识别或推断其情绪或意图目的的人工智能系统；

(40) “生物特征分类系统”指为根据自然人的生物特征数据将自然人归入特定类别目的的人工智能系统，除非该系统附属于另一商业服务且出于客观技术原因严格必要；

(41) “远程生物特征识别系统”指为识别自然人目的的人工智能系统，无需自然人主动参与，通常通过将某人的生物特征数据与参考数据库中包含的生物特征数据进行比较而在一定距离外进行；

(42) “实时远程生物特征识别系统”指生物特征数据的采集、比较和识别均无显著延迟地进行的远程生物特征识别系统，不仅包括即时识别，还包括有限的短暂延迟以避免规避；

(43) “事后远程生物特征识别系统”指实时远程生物特征识别系统以外的远程生物特征识别系统；

(44) “可公开进入的空间”指可供不特定数量的自然人进入的任何公有或私有物理场所，无论是否适用某些进入条件，也无论是否存在潜在容量限制；

(45) ‘law enforcement authority’ means:

(a) any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or

(b) any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

(46) ‘law enforcement’ means activities carried out by law enforcement authorities or on their behalf for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and preventing threats to public security;

(47) ‘AI Office’ means the Commission’s function of contributing to the implementation, monitoring and supervision of AI systems and general-purpose AI models, and AI governance, provided for in Commission Decision of 24 January 2024; references in this Regulation to the AI Office shall be construed as references to the Commission;

(48) ‘national competent authority’ means a notifying authority or a market surveillance authority; as regards AI systems put into service or used by Union institutions, agencies, offices and bodies, references to national competent authorities or market surveillance authorities in this Regulation shall be construed as references to the European Data Protection Supervisor;

(49) ‘serious incident’ means an incident or malfunctioning of an AI system that directly or indirectly leads to any of the following:

(a) the death of a person, or serious harm to a person’s health;

(b) a serious and irreversible disruption of the management or operation of critical infrastructure;

(c) the infringement of obligations under Union law intended to protect fundamental rights;

(d) serious harm to property or the environment;

(50) ‘personal data’ means personal data as defined in Article 4, point (1), of Regulation (EU) 2016/679;

(51) ‘non-personal data’ means data other than personal data as defined in Article 4, point (1), of Regulation (EU) 2016/679;

(52) ‘profiling’ means profiling as defined in Article 4, point (4), of Regulation (EU) 2016/679;

(53) ‘real-world testing plan’ means a document that describes the objectives, methodology, geographical, population and temporal scope, monitoring, organisation and conduct of testing in real-world conditions;

(54) ‘sandbox plan’ means a document agreed between the participating provider and the competent authority describing the objectives, conditions, timeframe, methodology and requirements for the activities carried out within the sandbox;

(55) ‘AI regulatory sandbox’ means a controlled framework set up by a competent authority which offers providers or prospective providers of AI systems the possibility to develop, train, validate and test, where appropriate in real-world conditions, an innovative AI system, pursuant to a sandbox plan for a limited time under regulatory supervision;

(56) ‘AI literacy’ means skills, knowledge and understanding that allow providers, deployers and affected persons, taking into account their respective rights and obligations in the context of this Regulation, to make an informed deployment of AI systems, as well as to gain awareness about the opportunities and risks of AI and possible harm it can cause;

(45) ‘执法机关’是指：

(a) 任何负责预防、调查、侦查或起诉刑事犯罪或执行刑事处罚，包括保障和预防对公共安全威胁的公共机构；或

(b) 任何其他由成员国法律授权为预防、调查、侦查或起诉刑事犯罪或执行刑事处罚，包括保障和预防对公共安全威胁的目的行使公共权力和公共权力的机构或实体；

(46) “执法”指执法机构或代表执法机构为预防、调查、侦查或起诉刑事犯罪或执行刑事处罚，包括保障和预防对公共安全威胁而开展的活动；

(47) “AI Office”指委员会根据2024年1月24日委员会决定所规定的、促进人工智能系统和通用人工智能模型的实施、监测和监督以及人工智能治理的职能；本条例中对AI Office的引用应解释为对委员会的引用；

(48) “国家主管机关”指通知机构或市场监督机构；对于由欧盟机构、机关、办公室和团体投入使用或使用的人工智能系统，本条例中对国家主管机关或市场监督机构的引用应解释为对欧洲数据保护监督员的引用；

(49) “严重事件”指直接或间接导致以下任何情形的人工智能系统事件或故障：

(a) 人员死亡，或对人员健康造成严重损害；

(b) 关键基础设施的管理或运营发生严重且不可逆的中断；

(c) 违反旨在保护基本权利的欧盟法律规定的义务；

(d) 对财产或环境造成严重损害；

(50) “个人数据”指Regulation(EU) 2016/679第4条第(1)点所定义的个人数据；

(51) “非个人数据”指Regulation(EU) 2016/679第4条第(1)点所定义的个人数据以外的数据；

(52) “画像”指第(EU) 2016/679号条例第4条第(4)点所定义的画像；

(53) “真实世界测试计划”指描述在真实世界条件下进行测试的目标、方法、地理、人口和时间范围、监测、组织和实施的文档；

(54) “沙盒计划”指参与提供者与主管机关之间达成的描述在沙盒内开展活动的目标、条件、时间框架、方法和要求的文档；

(55) “人工智能监管沙盒”指由主管机关建立的受控框架，为人工智能系统的提供者或潜在提供者提供在监管监督下，根据沙盒计划在有限时间内开发、训练、验证和测试(酌情在真实世界条件下)创新人工智能系统的可能性；

(56) “人工智能素养”指使提供者、部署者和受影响者(考虑到其在本条例背景下的各自权利和义务)能够知情地部署人工智能系统，以及了解人工智能的机遇和风险及其可能造成的损害的技能、知识和理解；

(57) 'testing in real-world conditions' means the temporary testing of an AI system for its intended purpose in real-world conditions outside a laboratory or otherwise simulated environment, with a view to gathering reliable and robust data and to assessing and verifying the conformity of the AI system with the requirements of this Regulation and it does not qualify as placing the AI system on the market or putting it into service within the meaning of this Regulation, provided that all the conditions laid down in Article 57 or 60 are fulfilled;

(58) 'subject', for the purpose of real-world testing, means a natural person who participates in testing in real-world conditions;

(59) 'informed consent' means a subject's freely given, specific, unambiguous and voluntary expression of his or her willingness to participate in a particular testing in real-world conditions, after having been informed of all aspects of the testing that are relevant to the subject's decision to participate;

(60) 'deep fake' means AI-generated or manipulated image, audio or video content that resembles existing persons, objects, places, entities or events and would falsely appear to a person to be authentic or truthful;

(61) 'widespread infringement' means any act or omission contrary to Union law protecting the interest of individuals, which:

(a) has harmed or is likely to harm the collective interests of individuals residing in at least two Member States other than the Member State in which:

(i) the act or omission originated or took place;

(ii) the provider concerned, or, where applicable, its authorised representative is located or established; or

(iii) the deployer is established, when the infringement is committed by the deployer;

(b) has caused, causes or is likely to cause harm to the collective interests of individuals and has common features, including the same unlawful practice or the same interest being infringed, and is occurring concurrently, committed by the same operator, in at least three Member States;

(62) 'critical infrastructure' means critical infrastructure as defined in Article 2, point (4), of Directive (EU) 2022/2557;

(63) 'general-purpose AI model' means an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market;

(64) 'high-impact capabilities' means capabilities that match or exceed the capabilities recorded in the most advanced general-purpose AI models;

(65) 'systemic risk' means a risk that is specific to the high-impact capabilities of general-purpose AI models, having a significant impact on the Union market due to their reach, or due to actual or reasonably foreseeable negative effects on public health, safety, public security, fundamental rights, or the society as a whole, that can be propagated at scale across the value chain;

(66) 'general-purpose AI system' means an AI system which is based on a general-purpose AI model and which has the capability to serve a variety of purposes, both for direct use as well as for integration in other AI systems;

(67) 'floating-point operation' means any mathematical operation or assignment involving floating-point numbers, which are a subset of the real numbers typically represented on computers by an integer of fixed precision scaled by an integer exponent of a fixed base;

(68) 'downstream provider' means a provider of an AI system, including a general-purpose AI system, which integrates an AI model, regardless of whether the AI model is provided by themselves and vertically integrated or provided by another entity based on contractual relations.

(57) "真实世界条件下的测试"是指在实验室或其他模拟环境之外，为预期目的在真实世界条件下对人工智能系统进行的临时测试，目的是收集可靠且稳健的数据，并评估和验证人工智能系统与本条例要求的符合性，且只要满足第57条或第60条规定的所有条件，该测试不构成本条例意义上的将人工智能系统投放市场或投入使用；

(58) "受试者"，就真实世界测试而言，指参与真实世界条件下测试的自然人；

(59) "知情同意"指受试者在被告知与受试者参与决定相关的测试所有方面后，自由给予、具体、明确且自愿地表示其愿意参与特定真实世界条件下测试；

(60) "深度伪造"指人工智能生成或操纵的图像、音频或视频内容，其类似于现有的人员、物体、地点、实体或事件，并且会虚假地使人看起来是真实的或真实的；

(61) "广泛侵权"指违反保护个人利益的欧盟法律的任何作为或不作为，其：

(a) 已经损害或可能损害居住在至少两个成员国的个人的集体利益，而非以下成员国：

(i) 作为或不作为起源或发生；

(ii) 相关提供者或(如适用)其授权代表所在或设立地；或

(iii) 部署者已设立，且侵权行为由该部署者实施时；

(b) 已经造成、正在造成或可能造成对个人集体利益的损害，并且具有共同特征，包括相同的非法行为或相同的利益受到侵害，并且由同一运营者在至少三个成员国同时发生；

(62) "关键基础设施"指Directive(EU) 2022/2557第2条第(4)点所定义的关键基础设施；

(63) "通用人工智能模型"是指一个人工智能模型，包括通过大规模自监督方式使用大量数据训练的人工智能模型，该模型表现出显著的通用性，能够胜任执行广泛的不同任务，无论该模型以何种方式投放市场，并且能够集成到各种下游系统或应用中，但在投放市场之前用于研究、开发或原型设计活动的人工智能模型除外；

(64) "高影响力能力"指匹配或超过最先进通用人工智能模型中记录的能力；

(65) "系统性风险"指通用人工智能模型的高影响力能力所特有的风险，由于其影响范围，或由于其可能对公共卫生、安全、公共安全、基本权利或整个社会产生的实际或合理可预见的负面影响，而在整个价值链上大规模传播，从而对欧盟市场产生重大影响；

(66) "通用人工智能系统"指基于通用人工智能模型的人工智能系统，其具有服务于多种用途的能力，既可直接使用，也可集成到其他人工智能系统中；

(67) "浮点运算"指涉及浮点数的任何数学运算或赋值，浮点数是实数的一个子集，通常在计算机上由固定精度的整数乘以固定基数的整数指数表示；

(68) "下游提供者"指集成人工智能模型的人工智能系统(包括通用人工智能系统)的提供者，无论该人工智能模型是由其自己提供并垂直集成，还是由另一实体基于合同关系提供。

Article 4

AI literacy

Providers and deployers of AI systems shall take measures to ensure, to their best extent, a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used.

CHAPTER II

PROHIBITED AI PRACTICES

Article 5

Prohibited AI practices

1. The following AI practices shall be prohibited:

(a) the placing on the market, the putting into service or the use of an AI system that deploys subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective, or the effect of materially distorting the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision, thereby causing them to take a decision that they would not have otherwise taken in a manner that causes or is reasonably likely to cause that person, another person or group of persons significant harm;

(b) the placing on the market, the putting into service or the use of an AI system that exploits any of the vulnerabilities of a natural person or a specific group of persons due to their age, disability or a specific social or economic situation, with the objective, or the effect, of materially distorting the behaviour of that person or a person belonging to that group in a manner that causes or is reasonably likely to cause that person or another person significant harm;

(c) the placing on the market, the putting into service or the use of AI systems for the evaluation or classification of natural persons or groups of persons over a certain period of time based on their social behaviour or known, inferred or predicted personal or personality characteristics, with the social score leading to either or both of the following:

(i) detrimental or unfavourable treatment of certain natural persons or groups of persons in social contexts that are unrelated to the contexts in which the data was originally generated or collected;

(ii) detrimental or unfavourable treatment of certain natural persons or groups of persons that is unjustified or disproportionate to their social behaviour or its gravity;

(d) the placing on the market, the putting into service for this specific purpose, or the use of an AI system for making risk assessments of natural persons in order to assess or predict the risk of a natural person committing a criminal offence, based solely on the profiling of a natural person or on assessing their personality traits and characteristics; this prohibition shall not apply to AI systems used to support the human assessment of the involvement of a person in a criminal activity, which is already based on objective and verifiable facts directly linked to a criminal activity;

(e) the placing on the market, the putting into service for this specific purpose, or the use of AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage;

(f) the placing on the market, the putting into service for this specific purpose, or the use of AI systems to infer emotions of a natural person in the areas of workplace and education institutions, except where the use of the AI system is intended to be put in place or into the market for medical or safety reasons;

第4条

AI 素养

人工智能系统的提供者和部署者应采取措施，尽最大努力确保其工作人员以及代表其处理人工智能系统操作和使用的其他人员具备足够的人工智能素养，同时考虑其技术知识、经验、教育和培训以及人工智能系统将要使用的场景，并考虑人工智能系统将要作用于的人员或群体。

第二章

被禁止的人工智能实践

第5条

禁止的人工智能实践

1. 以下人工智能实践应被禁止：

(a) 将部署超越人的意识的潜意识技术或有目的操纵或欺骗技术的人工智能系统投放市场、投入使用或使用该人工智能系统，其目的或效果是通过显著损害一个人或一群人的知情决策能力，从而实质性扭曲其行为，致使他们以否则不会采取的方式作出决定，从而对该人、另一人或一群人造成或合理可能造成重大损害；

(b) 投放市场、投入使用或使用利用自然人因年龄、残疾或特定社会或经济状况而具有的任何脆弱性的人工智能系统，其目的或效果是实质性扭曲该人或属于该群体的个人的行为，从而对该人或另一人造成或合理可能造成重大损害；

(c) 投放市场、投入使用或使用人工智能系统，在一定时期内基于自然人或群体的社会行为或已知、推断或预测的个人或人格特征对其进行评估或分类，社会评分导致以下任一或两种情况：

(i) 在与数据最初生成或收集的背景无关的社会背景下，对某些自然人或群体造成不利或不利待遇；

(ii) 对某些自然人或者群体因其社会行为或者该行为的严重程度而给予的没有正当理由或者不成比例的、有害的或者不利的待遇；

(d) 将人工智能系统投放市场、为该特定目的投入使用或使用人工智能系统，对自然人进行风险评估，以仅基于对自然人的特征分析或评估其人格特质和特征来评估或预测自然人实施刑事犯罪的风险；本禁令不适用于用于支持人工评估某人是否参与犯罪活动的人工智能系统，该评估已基于与犯罪活动直接相关的客观且可核实的事实；

(e) 投放市场、为此特定目的投入使用或者使用通过从互联网或者闭路电视录像中无针对性地抓取面部图像来创建或者扩充面部识别数据库的人工智能系统；

(f) 在工作场所和教育机构领域，投放市场、为此特定目的投入使用或者使用推断自然人情緒的人工智能系统，但该人工智能系统的使用系出于医疗或者安全原因而拟设立或者投放市场的除外；

(g) the placing on the market, the putting into service for this specific purpose, or the use of biometric categorisation systems that categorise individually natural persons based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation; this prohibition does not cover any labelling or filtering of lawfully acquired biometric datasets, such as images, based on biometric data or categorizing of biometric data in the area of law enforcement;

(h) the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement, unless and in so far as such use is strictly necessary for one of the following objectives:

(i) the targeted search for specific victims of abduction, trafficking in human beings or sexual exploitation of human beings, as well as the search for missing persons;

(ii) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attack;

(iii) the localisation or identification of a person suspected of having committed a criminal offence, for the purpose of conducting a criminal investigation or prosecution or executing a criminal penalty for offences referred to in Annex II and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least four years.

Point (h) of the first subparagraph is without prejudice to Article 9 of Regulation (EU) 2016/679 for the processing of biometric data for purposes other than law enforcement.

2. The use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement for any of the objectives referred to in paragraph 1, first subparagraph, point (h), shall be deployed for the purposes set out in that point only to confirm the identity of the specifically targeted individual, and it shall take into account the following elements:

(a) the nature of the situation giving rise to the possible use, in particular the seriousness, probability and scale of the harm that would be caused if the system were not used;

(b) the consequences of the use of the system for the rights and freedoms of all persons concerned, in particular the seriousness, probability and scale of those consequences.

In addition, the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement for any of the objectives referred to in paragraph 1, first subparagraph, point (h), of this Article shall comply with necessary and proportionate safeguards and conditions in relation to the use in accordance with the national law authorising the use thereof, in particular as regards the temporal, geographic and personal limitations. The use of the 'real-time' remote biometric identification system in publicly accessible spaces shall be authorised only if the law enforcement authority has completed a fundamental rights impact assessment as provided for in Article 27 and has registered the system in the EU database according to Article 49. However, in duly justified cases of urgency, the use of such systems may be commenced without the registration in the EU database, provided that such registration is completed without undue delay.

3. For the purposes of paragraph 1, first subparagraph, point (h) and paragraph 2, each use for the purposes of law enforcement of a 'real-time' remote biometric identification system in publicly accessible spaces shall be subject to a prior authorisation granted by a judicial authority or an independent administrative authority whose decision is binding of the Member State in which the use is to take place, issued upon a reasoned request and in accordance with the detailed rules of national law referred to in paragraph 5. However, in a duly justified situation of urgency, the use of such system may be commenced without an authorisation provided that such authorisation is requested without undue delay, at the latest within 24 hours. If such authorisation is rejected, the use shall be stopped with immediate effect and all the data, as well as the results and outputs of that use shall be immediately discarded and deleted.

The competent judicial authority or an independent administrative authority whose decision is binding shall grant the authorisation only where it is satisfied, on the basis of objective evidence or clear indications presented to it, that the use of the 'real-time' remote biometric identification system concerned is necessary for, and proportionate to, achieving one of the

(g) 将生物特征分类系统投放市场、为该特定目的投入使用或使用该系统，该系统基于自然人的生物特征数据对自然人进行个体分类，以推断或推测其种族、政治观点、工会成员身份、宗教或哲学信仰、性生活或性取向；本禁令不涵盖对合法获取的生物特征数据集(如图像)基于生物特征数据进行的任何标注或过滤，也不涵盖执法领域对生物特征数据的分类；

(h) 在可公开进入的空间中为执法目的使用"实时"远程生物特征识别系统，除非且仅限于此种使用对于下列目标之一属严格必要：

(i) 有针对性地搜寻特定的绑架、人口贩运或者性剥削受害者，以及搜寻失踪人员；

(ii) 防止对自然人的生命或者人身安全构成特定的、重大的和迫在眉睫的威胁，或者防止真实且当前存在或者真实且可预见的恐怖袭击威胁；

(iii) 对涉嫌实施刑事犯罪的人员进行定位或者识别，以就附件II所列且在有关成员国可处以最高至少四年监禁或者拘留令的犯罪进行刑事侦查或者起诉或者执行刑事处罚。

第一项第(h)点不影响 Regulation (EU) 2016/679 第 9 条关于为执法以外目的处理生物特征数据的规定。

2. 在可公开进入的空间中为执法目的、为第1款第一项第(h)点所述任何目标而使用"实时"远程生物特征识别系统，仅应为该点所规定之目的进行部署，以确认特定目标个人的身份，并应考虑下列要素：

(a) 引发可能使用之情形的性质，特别是若不使用该系统将造成的损害的严重性、可能性和规模；

(b) 使用该系统对所有相关人员的权利和自由造成的后果，特别是该等后果的严重性、可能性和规模。

此外，为执法目的在公开可访问空间中使用"实时"远程生物特征识别系统以实现本条第1款第一项第(h)点所述任何目标，应当遵守根据授权使用该系统的国家法律所规定的必要且相称的保障措施和条件，特别是关于时间、地域和个人限制方面。"实时"远程生物特征识别系统在公开可访问空间中的使用，仅在执法机构已完成第27条规定的基本权利影响评估并根据第49条将该系统登记在EU数据库中的情况下，方应获得授权。然而，在有正当理由的紧急情况下，此类系统的使用可在未在EU数据库登记的情况下开始，前提是该登记无不合理延迟地完成。

3. 为第1款第一项第(h)点和第2款的目的，为执法目的在公开可访问空间中使用"实时"远程生物特征识别系统，每次使用均应获得使用发生地成员国司法机构或独立行政机构(其决定具有约束力)的事先授权，该授权应基于附理由的请求并根据第5款所述国家法律的详细规则签发。然而，在有正当理由的紧急情况下，此类系统的使用可在未获授权的情况下开始，前提是无不合理延迟地请求该授权，最迟在24小时内。如该授权被拒绝，使用应立即停止，该使用的所有数据以及结果和输出应立即丢弃和删除。

主管司法机关或者其决定具有约束力的独立行政机关，只有在根据向其提交的客观证据或者明确迹象确信有关"实时"远程生物特征识别系统的使用对于实现下列目标之一属必要且相称时，方可予以授权

objectives specified in paragraph 1, first subparagraph, point (h), as identified in the request and, in particular, remains limited to what is strictly necessary concerning the period of time as well as the geographic and personal scope. In deciding on the request, that authority shall take into account the elements referred to in paragraph 2. No decision that produces an adverse legal effect on a person may be taken based solely on the output of the 'real-time' remote biometric identification system.

4. Without prejudice to paragraph 3, each use of a 'real-time' remote biometric identification system in publicly accessible spaces for law enforcement purposes shall be notified to the relevant market surveillance authority and the national data protection authority in accordance with the national rules referred to in paragraph 5. The notification shall, as a minimum, contain the information specified under paragraph 6 and shall not include sensitive operational data.

5. A Member State may decide to provide for the possibility to fully or partially authorise the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement within the limits and under the conditions listed in paragraph 1, first subparagraph, point (h), and paragraphs 2 and 3. Member States concerned shall lay down in their national law the necessary detailed rules for the request, issuance and exercise of, as well as supervision and reporting relating to, the authorisations referred to in paragraph 3. Those rules shall also specify in respect of which of the objectives listed in paragraph 1, first subparagraph, point (h), including which of the criminal offences referred to in point (h)(iii) thereof, the competent authorities may be authorised to use those systems for the purposes of law enforcement. Member States shall notify those rules to the Commission at the latest 30 days following the adoption thereof. Member States may introduce, in accordance with Union law, more restrictive laws on the use of remote biometric identification systems.

6. National market surveillance authorities and the national data protection authorities of Member States that have been notified of the use of 'real-time' remote biometric identification systems in publicly accessible spaces for law enforcement purposes pursuant to paragraph 4 shall submit to the Commission annual reports on such use. For that purpose, the Commission shall provide Member States and national market surveillance and data protection authorities with a template, including information on the number of the decisions taken by competent judicial authorities or an independent administrative authority whose decision is binding upon requests for authorisations in accordance with paragraph 3 and their result.

7. The Commission shall publish annual reports on the use of real-time remote biometric identification systems in publicly accessible spaces for law enforcement purposes, based on aggregated data in Member States on the basis of the annual reports referred to in paragraph 6. Those annual reports shall not include sensitive operational data of the related law enforcement activities.

8. This Article shall not affect the prohibitions that apply where an AI practice infringes other Union law.

CHAPTER III

HIGH-RISK AI SYSTEMS

SECTION 1

Classification of AI systems as high-risk

Article 6

Classification rules for high-risk AI systems

1. Irrespective of whether an AI system is placed on the market or put into service independently of the products referred to in points (a) and (b), that AI system shall be considered to be high-risk where both of the following conditions are fulfilled:

(a) the AI system is intended to be used as a safety component of a product, or the AI system is itself a product, covered by the Union harmonisation legislation listed in Annex I;

(b) the product whose safety component pursuant to point (a) is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment, with a view to the placing on the market or the putting into service of that product pursuant to the Union harmonisation legislation listed in Annex I.

2. In addition to the high-risk AI systems referred to in paragraph 1, AI systems referred to in Annex III shall be considered to be high-risk.

请求中所确定的第1款第一项第(h)点规定的目标，并且特别是在时间期限以及地域和个人范围方面，保持在严格必要的限度内。在决定该请求时，该机构应考虑第2款所述要素。不得仅基于"实时"远程生物特征识别系统的输出作出对个人产生不利法律效果的决定。

4. 在不影响第3款的情况下，在可公开进入的空间中为执法目的每次使用"实时"远程生物特征识别系统，均应依照第5款所述国家规则通知相关市场监督机构和国家数据保护机构。该通知至少应包含第6款规定的信息，且不得包含敏感行动数据。

5. 成员国可决定规定，在第1款第一项第(h)点以及第2款和第3款所列限制和条件下，完全或部分授权为执法目的在公开可访问空间中使用"实时"远程生物特征识别系统的可能性。有关成员国应在其国家法律中规定请求、签发和行使第3款所述授权以及与之相关的监督和报告所需的详细规则。这些规则还应明确，主管机构可被授权为执法目的使用这些系统针对第1款第一项第(h)点所列哪些目标，包括其第(h)点第(iii)项所述哪些刑事犯罪。成员国应最迟在通过这些规则后30天内通知委员会。成员国可根据欧盟法律，就远程生物特征识别系统的使用引入更严格的国内法。

6. 已根据第4款获知为执法目的在公开可访问空间中使用"实时"远程生物特征识别系统的成员国国家市场监督机构和国家数据保护机构，应向委员会提交关于此类使用的年度报告。为此，委员会应向成员国和国家市场监督及数据保护机构提供模板，包括关于主管司法机构或独立行政机构(其决定具有约束力)根据第3款对授权请求所作决定的数量及其结果的信息。

7. 委员会应根据成员国依据第6款所述年度报告汇总的数据，发布关于在可公开进入的空间中为执法目的使用实时远程生物特征识别系统的年度报告。该等年度报告不得包含相关执法活动的敏感行动数据。

8. 本条不影响在人工智能实践违反其他欧盟法律时适用的禁止性规定。

第三章

高风险人工智能系统

第1节

将人工智能系统分类为高风险

第6条

高风险人工智能系统的分类规则

1. 无论人工智能系统是否独立于第(a)项和第(b)点所述产品投放市场或者投入使用，在同时满足下列两项条件时，该人工智能系统应被视为高风险：

(a) 该人工智能系统拟作为产品的安全组件使用，或者该人工智能系统本身即为附件I所列欧盟协调立法所涵盖的产品；

(b) 根据第(a)项其安全组件为该人工智能系统的产品，或者作为产品的人工智能系统本身，须依照附件I所列欧盟协调立法就该产品的投放市场或者投入使用进行第三方合格评定。

2. 除第1款所述高风险人工智能系统外，附件III所述人工智能系统也应被视为高风险。

3. By derogation from paragraph 2, an AI system referred to in Annex III shall not be considered to be high-risk where it does not pose a significant risk of harm to the health, safety or fundamental rights of natural persons, including by not materially influencing the outcome of decision making.

The first subparagraph shall apply where any of the following conditions is fulfilled:

(a) the AI system is intended to perform a narrow procedural task;

(b) the AI system is intended to improve the result of a previously completed human activity;

(c) the AI system is intended to detect decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment, without proper human review; or

(d) the AI system is intended to perform a preparatory task to an assessment relevant for the purposes of the use cases listed in Annex III.

Notwithstanding the first subparagraph, an AI system referred to in Annex III shall always be considered to be high-risk where the AI system performs profiling of natural persons.

4. A provider who considers that an AI system referred to in Annex III is not high-risk shall document its assessment before that system is placed on the market or put into service. Such provider shall be subject to the registration obligation set out in Article 49(2). Upon request of national competent authorities, the provider shall provide the documentation of the assessment.

5. The Commission shall, after consulting the European Artificial Intelligence Board (the 'Board'), and no later than 2 February 2026, provide guidelines specifying the practical implementation of this Article in line with Article 96 together with a comprehensive list of practical examples of use cases of AI systems that are high-risk and not high-risk.

6. The Commission is empowered to adopt delegated acts in accordance with Article 97 in order to amend paragraph 3, second subparagraph, of this Article by adding new conditions to those laid down therein, or by modifying them, where there is concrete and reliable evidence of the existence of AI systems that fall under the scope of Annex III, but do not pose a significant risk of harm to the health, safety or fundamental rights of natural persons.

7. The Commission shall adopt delegated acts in accordance with Article 97 in order to amend paragraph 3, second subparagraph, of this Article by deleting any of the conditions laid down therein, where there is concrete and reliable evidence that this is necessary to maintain the level of protection of health, safety and fundamental rights provided for by this Regulation.

8. Any amendment to the conditions laid down in paragraph 3, second subparagraph, adopted in accordance with paragraphs 6 and 7 of this Article shall not decrease the overall level of protection of health, safety and fundamental rights provided for by this Regulation and shall ensure consistency with the delegated acts adopted pursuant to Article 7(1), and take account of market and technological developments.

Article 7

Amendments to Annex III

1. The Commission is empowered to adopt delegated acts in accordance with Article 97 to amend Annex III by adding or modifying use-cases of high-risk AI systems where both of the following conditions are fulfilled:

(a) the AI systems are intended to be used in any of the areas listed in Annex III;

(b) the AI systems pose a risk of harm to health and safety, or an adverse impact on fundamental rights, and that risk is equivalent to, or greater than, the risk of harm or of adverse impact posed by the high-risk AI systems already referred to in Annex III.

3. 作为对第2款的减损，附件III所述人工智能系统在不对自然人的健康、安全或者基本权利构成重大损害风险时，包括未对决策结果产生实质性影响时，不应被视为高风险。

第一小段在满足以下任一条件时适用：

(a) AI 系统的意图是执行一项狭窄的程序性任务；

(b) 该人工智能系统旨在改进先前已完成的人类活动的结果；

(c) 该人工智能系统旨在检测决策模式或者与先前决策模式的偏差，且在没有适当人类审查的情况下，并非旨在取代或者影响先前已完成的人类评估；或者

(d) 该人工智能系统旨在执行为附件III所列用例之目的相关评估的预备性任务。

尽管有第一小段的规定，附件三所述人工智能系统在该人工智能系统对自然人进行画像时，应始终被视为高风险。

4. 认为附件III所述人工智能系统并非高风险的提供者，应在该系统投放市场或者投入使用之前记录其评估。该提供者应遵守第49条第2款规定的登记义务。应国家主管机关的要求，提供者应提供该评估的文件。

5. 委员会应在咨询欧洲人工智能委员会("委员会")后，至迟于2026年2月2日，依照第96条提供明确本条实际实施的指南，并附上高风险和非高风险人工智能系统用例的全面实用示例清单。

6. 委员会有权依照第97条通过授权法案，以在有具体且可靠证据表明存在属于附件III范围但不对自然人的健康、安全或者基本权利构成重大损害风险的人工智能系统时，通过向本条第3款第二项所述条件中增加新条件或者修改该等条件来修订该款。

7. 委员会应依照第97条通过授权法案，以在有具体且可靠证据表明为维持本条例所规定的健康、安全和基本权利保护水平而有必要时，通过删除本条第3款第二项所述任何条件来修订该款。

8. 依照本条第6款和第7款通过的对第3款第二项所述条件的任何修订，不得降低本条例所规定的健康、安全和基本权利的整体保护水平，并应确保与依照第7条第1款通过的授权法案保持一致，且应考虑市场和技术发展。

第7条

对附件三的修订

1. 委员会有权依照第97条通过授权法案，以在同时满足下列两项条件时，通过增加或者修改高风险人工智能系统的用例来修订附件III:

(a) AI系统拟用于Annex III所列的任何领域；

(b) 该等人工智能系统对健康和安全构成损害风险，或者对基本权利产生不利影响，且该风险等同于或者大于附件III已述高风险人工智能系统所造成的损害风险或者不利影响。

2. When assessing the condition under paragraph 1, point (b), the Commission shall take into account the following criteria:

(a) the intended purpose of the AI system;

(b) the extent to which an AI system has been used or is likely to be used;

(c) the nature and amount of the data processed and used by the AI system, in particular whether special categories of personal data are processed;

(d) the extent to which the AI system acts autonomously and the possibility for a human to override a decision or recommendations that may lead to potential harm;

(e) the extent to which the use of an AI system has already caused harm to health and safety, has had an adverse impact on fundamental rights or has given rise to significant concerns in relation to the likelihood of such harm or adverse impact, as demonstrated, for example, by reports or documented allegations submitted to national competent authorities or by other reports, as appropriate;

(f) the potential extent of such harm or such adverse impact, in particular in terms of its intensity and its ability to affect multiple persons or to disproportionately affect a particular group of persons;

(g) the extent to which persons who are potentially harmed or suffer an adverse impact are dependent on the outcome produced with an AI system, in particular because for practical or legal reasons it is not reasonably possible to opt-out from that outcome;

(h) the extent to which there is an imbalance of power, or the persons who are potentially harmed or suffer an adverse impact are in a vulnerable position in relation to the deployer of an AI system, in particular due to status, authority, knowledge, economic or social circumstances, or age;

(i) the extent to which the outcome produced involving an AI system is easily corrigible or reversible, taking into account the technical solutions available to correct or reverse it, whereby outcomes having an adverse impact on health, safety or fundamental rights, shall not be considered to be easily corrigible or reversible;

(j) the magnitude and likelihood of benefit of the deployment of the AI system for individuals, groups, or society at large, including possible improvements in product safety;

(k) the extent to which existing Union law provides for:

(i) effective measures of redress in relation to the risks posed by an AI system, with the exclusion of claims for damages;

(ii) effective measures to prevent or substantially minimise those risks.

3. The Commission is empowered to adopt delegated acts in accordance with Article 97 to amend the list in Annex III by removing high-risk AI systems where both of the following conditions are fulfilled:

(a) the high-risk AI system concerned no longer poses any significant risks to fundamental rights, health or safety, taking into account the criteria listed in paragraph 2;

(b) the deletion does not decrease the overall level of protection of health, safety and fundamental rights under Union law.

SECTION 2

Requirements for high-risk AI systems

Article 8

Compliance with the requirements

1. High-risk AI systems shall comply with the requirements laid down in this Section, taking into account their intended purpose as well as the generally acknowledged state of the art on AI and AI-related technologies. The risk management system referred to in Article 9 shall be taken into account when ensuring compliance with those requirements.

2. 在评估第1款第(b)项所述条件时，委员会应考虑下列标准：

(a) AI系统的预期目的；

(b) AI 系统已被使用或可能被使用的程度；

(c) 人工智能系统处理和使用的数据的性质与数量，特别是是否处理特殊类别的个人数据；

(d) 人工智能系统自主行动的程度，以及人类推翻可能导致潜在损害的决策或建议的可能性；

(e) 人工智能系统的使用已经对健康和安全造成损害、对基本权利产生不利影响，或引起对这类损害或不利影响可能性的重大关切的程度，例如通过提交给国家主管机关的报告或记录在案的指控或其他报告(视情况而定)所证明的；

(f) 此类损害或此类不利影响的潜在程度，特别是就其强度及其影响多人的能力或对特定人群造成不成比例影响的能力而言；

(g) 可能受到损害或遭受不利影响的人对人工智能系统所产生结果的依赖程度，特别是因为出于实际或法律原因，合理地不可能选择退出该结果；

(h) 权力不平衡的程度，或可能受到损害或遭受不利影响的人相对于人工智能系统部署者处于弱势地位的程度，特别是由于地位、权威、知识、经济或社会状况或年龄；

(i) 涉及人工智能系统所产生结果易于纠正或逆转的程度，同时考虑到可用于纠正或逆转该结果的技术解决方案，其中对健康、安全或基本权利产生不利影响的结果不得被视为易于纠正或逆转；

(j) 部署人工智能系统对个人、群体或整个社会的好处的规模和可能性，包括产品安全的可能改进；

(k) 现行欧盟法律在多大程度上规定了：

(i) 针对人工智能系统所构成风险的有效救济措施，损害赔偿请求除外；

(ii) 防止或大幅降低这些风险的有效措施。

3. 委员会有权根据第97条通过授权法案，在满足以下两项条件时，通过移除高风险人工智能系统来修订Annex III中的清单：

(a) 考虑到第2款所列标准，相关高风险人工智能系统不再对基本权利、健康或安全构成任何重大风险；

(b) 删除不会降低欧盟法律下对健康、安全和基本权利的整体保护水平。

第2节

高风险人工智能系统的要求

第8条

符合要求

1. 高风险人工智能系统应遵守本节规定的要求，同时考虑其预期用途以及人工智能和人工智能相关技术公认的最新水平。在确保遵守这些要求时，应考虑第9条所述的风险管理体系。

2. Where a product contains an AI system, to which the requirements of this Regulation as well as requirements of the Union harmonisation legislation listed in Section A of Annex I apply, providers shall be responsible for ensuring that their product is fully compliant with all applicable requirements under applicable Union harmonisation legislation. In ensuring the compliance of high-risk AI systems referred to in paragraph 1 with the requirements set out in this Section, and in order to ensure consistency, avoid duplication and minimise additional burdens, providers shall have a choice of integrating, as appropriate, the necessary testing and reporting processes, information and documentation they provide with regard to their product into documentation and procedures that already exist and are required under the Union harmonisation legislation listed in Section A of Annex I.

Article 9

Risk management system

1. A risk management system shall be established, implemented, documented and maintained in relation to high-risk AI systems.

2. The risk management system shall be understood as a continuous iterative process planned and run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic review and updating. It shall comprise the following steps:

(a) the identification and analysis of the known and the reasonably foreseeable risks that the high-risk AI system can pose to health, safety or fundamental rights when the high-risk AI system is used in accordance with its intended purpose;

(b) the estimation and evaluation of the risks that may emerge when the high-risk AI system is used in accordance with its intended purpose, and under conditions of reasonably foreseeable misuse;

(c) the evaluation of other risks possibly arising, based on the analysis of data gathered from the post-market monitoring system referred to in Article 72;

(d) the adoption of appropriate and targeted risk management measures designed to address the risks identified pursuant to point (a).

3. The risks referred to in this Article shall concern only those which may be reasonably mitigated or eliminated through the development or design of the high-risk AI system, or the provision of adequate technical information.

4. The risk management measures referred to in paragraph 2, point (d), shall give due consideration to the effects and possible interaction resulting from the combined application of the requirements set out in this Section, with a view to minimising risks more effectively while achieving an appropriate balance in implementing the measures to fulfil those requirements.

5. The risk management measures referred to in paragraph 2, point (d), shall be such that the relevant residual risk associated with each hazard, as well as the overall residual risk of the high-risk AI systems is judged to be acceptable.

In identifying the most appropriate risk management measures, the following shall be ensured:

(a) elimination or reduction of risks identified and evaluated pursuant to paragraph 2 in as far as technically feasible through adequate design and development of the high-risk AI system;

(b) where appropriate, implementation of adequate mitigation and control measures addressing risks that cannot be eliminated;

(c) provision of information required pursuant to Article 13 and, where appropriate, training to deployers.

With a view to eliminating or reducing risks related to the use of the high-risk AI system, due consideration shall be given to the technical knowledge, experience, education, the training to be expected by the deployer, and the presumable context in which the system is intended to be used.

2. 当产品包含人工智能系统，且本法规的要求以及附件一A节所列欧盟协调立法的要求适用于该产品时，提供者应负责确保其产品完全符合适用欧盟协调立法下的所有适用要求。在确保第1款所述高风险人工智能系统符合本节规定的要求时，为确保一致性、避免重复并尽量减少额外负担，提供者应有权酌情将其就产品提供的必要测试和报告流程、信息和文档整合到附件一A节所列欧盟协调立法下已存在且要求的文档和程序中。

第9条

风险管理系统

1. 应针对高风险人工智能系统建立、实施、记录和维护风险管理体系。

2. 风险管理体系应被理解为在高风险人工智能系统整个生命周期内计划和运行的持续迭代过程，需要定期系统审查和更新。其应包括以下步骤：

(a) 识别和分析高风险人工智能系统在按照其预期用途使用时可能对健康、安全或基本权利构成的已知风险和可合理预见风险；

(b) 估计和评估高风险人工智能系统在按照其预期用途使用以及在可合理预见的误用条件下可能出现的风险；

(c) 基于对第72条所述上市后监测系统所收集数据的分析，评估可能产生的其他风险；

(d) 采取适当且有针对性、旨在应对依据第(a)点所识别风险的风险管理措施。

3. 本条所述风险仅应涉及可通过高风险人工智能系统的开发或设计，或通过提供适当技术信息而可合理缓解或消除的风险。

4. 第2款第(d)点所述风险管理措施应适当考虑本节所列要求综合适用所产生的效果和可能的相互作用，以便更有效地最小化风险，同时在实施满足这些要求的措施时实现适当平衡。

5. 第2款第(d)点所述风险管理措施应使与每种危害相关的相关剩余风险以及高风险人工智能系统的整体剩余风险被判定为可接受。

在确定最适当的风险管理措施时，应确保以下各项：

(a) 在技术可行的范围内，通过高风险人工智能系统的适当设计和开发，消除或减少依据第2款所识别和评估的风险；

(b) 酌情实施适当的缓解和控制措施，以应对无法消除的风险；

(c) 提供依据第13条所需的信息，并酌情向部署者提供培训。

为消除或减少与使用高风险人工智能系统相关的风险，应适当考虑部署者可预期的技术知识、经验、教育、培训，以及系统预期使用的大致情境。

6. High-risk AI systems shall be tested for the purpose of identifying the most appropriate and targeted risk management measures. Testing shall ensure that high-risk AI systems perform consistently for their intended purpose and that they are in compliance with the requirements set out in this Section.

7. Testing procedures may include testing in real-world conditions in accordance with Article 60.

8. The testing of high-risk AI systems shall be performed, as appropriate, at any time throughout the development process, and, in any event, prior to their being placed on the market or put into service. Testing shall be carried out against prior defined metrics and probabilistic thresholds that are appropriate to the intended purpose of the high-risk AI system.

9. When implementing the risk management system as provided for in paragraphs 1 to 7, providers shall give consideration to whether in view of its intended purpose the high-risk AI system is likely to have an adverse impact on persons under the age of 18 and, as appropriate, other vulnerable groups.

10. For providers of high-risk AI systems that are subject to requirements regarding internal risk management processes under other relevant provisions of Union law, the aspects provided in paragraphs 1 to 9 may be part of, or combined with, the risk management procedures established pursuant to that law.

Article 10

Data and data governance

1. High-risk AI systems which make use of techniques involving the training of AI models with data shall be developed on the basis of training, validation and testing data sets that meet the quality criteria referred to in paragraphs 2 to 5 whenever such data sets are used.

2. Training, validation and testing data sets shall be subject to data governance and management practices appropriate for the intended purpose of the high-risk AI system. Those practices shall concern in particular:

(a) the relevant design choices;

(b) data collection processes and the origin of data, and in the case of personal data, the original purpose of the data collection;

(c) relevant data-preparation processing operations, such as annotation, labelling, cleaning, updating, enrichment and aggregation;

(d) the formulation of assumptions, in particular with respect to the information that the data are supposed to measure and represent;

(e) an assessment of the availability, quantity and suitability of the data sets that are needed;

(f) examination in view of possible biases that are likely to affect the health and safety of persons, have a negative impact on fundamental rights or lead to discrimination prohibited under Union law, especially where data outputs influence inputs for future operations;

(g) appropriate measures to detect, prevent and mitigate possible biases identified according to point (f);

(h) the identification of relevant data gaps or shortcomings that prevent compliance with this Regulation, and how those gaps and shortcomings can be addressed.

3. Training, validation and testing data sets shall be relevant, sufficiently representative, and to the best extent possible, free of errors and complete in view of the intended purpose. They shall have the appropriate statistical properties, including, where applicable, as regards the persons or groups of persons in relation to whom the high-risk AI system is intended to be used. Those characteristics of the data sets may be met at the level of individual data sets or at the level of a combination thereof.

4. Data sets shall take into account, to the extent required by the intended purpose, the characteristics or elements that are particular to the specific geographical, contextual, behavioural or functional setting within which the high-risk AI system is intended to be used.

6. 应对高风险人工智能系统进行测试，以识别最适当且有针对性风险管理措施。测试应确保高风险人工智能系统按其预期用途持续运行，并确保其符合本节规定的要求。

7. 测试程序可包括按照第60条在真实世界条件下进行测试。

8. 高风险人工智能系统的测试应酌情在开发过程中的任何时候进行，并且在任何情况下均应在投放市场或投入使用之前进行。测试应针对适合高风险人工智能系统预期用途的预先定义的指标和概率阈值进行。

9. 在实施第1至7款规定的风险管理体系时，提供者应考虑鉴于其预期用途，高风险人工智能系统是否可能对18岁以下人员以及酌情对其他弱势群体产生不利影响。

10. 对于受欧盟法律其他相关条款下内部风险管理流程要求约束的高风险人工智能系统提供者，第1至9款规定的方面可构成依据该法律建立的风险管理程序的一部分，或与之结合。

第10条

数据与数据治理

1. 利用涉及以数据训练人工智能模型的技术的高风险人工智能系统，在使用了此类数据集的情况下，应基于符合第2至第5段所述质量标准的数据集进行训练、验证和测试来开发。

2. 训练、验证和测试数据集应遵守适合高风险人工智能系统预期目的的数据治理和管理实践。这些实践尤其应涉及：

(a) 相关设计选择；

(b) 数据收集过程和数据来源，以及在个人数据的情况下，数据收集的原始目的；

(c) 相关的数据准备处理操作，如注释、标注、清理、更新、丰富和聚合；

(d) 假设的制定，特别是关于数据应衡量和表示的信息；

(e) 对所需数据集的可用性、数量和适用性的评估；

(f) 针对可能影响人员健康和安全、对基本权利产生负面影响或导致欧盟法律所禁止的歧视的可能偏见进行审查，特别是在数据输出影响未来操作的输入的情况下；

(g) 采取适当措施以检测、预防和减轻根据第(f)点识别的可能偏见；(h) 识别妨碍遵守本条例的相关数据缺口或缺陷，以及如何解决这些缺口和缺陷。

3. 训练、验证和测试数据集应相关、具有充分代表性，并尽可能在预期目的方面无错误且完整。它们应具有适当的统计特性，包括在适用情况下，涉及高风险人工智能系统预期使用所针对的人员或人员群体方面的统计特性。数据集的这些特性可在单个数据集层面或其组合层面满足。

4. 数据集应在预期目的所需的范围内，考虑高风险人工智能系统预期使用所在特定地理、背景、行为或功能环境的特征或要素。

5. To the extent that it is strictly necessary for the purpose of ensuring bias detection and correction in relation to the high-risk AI systems in accordance with paragraph (2), points (f) and (g) of this Article, the providers of such systems may exceptionally process special categories of personal data, subject to appropriate safeguards for the fundamental rights and freedoms of natural persons. In addition to the provisions set out in Regulations (EU) 2016/679 and (EU) 2018/1725 and Directive (EU) 2016/680, all the following conditions must be met in order for such processing to occur:

(a) the bias detection and correction cannot be effectively fulfilled by processing other data, including synthetic or anonymised data;

(b) the special categories of personal data are subject to technical limitations on the re-use of the personal data, and state-of-the-art security and privacy-preserving measures, including pseudonymisation;

(c) the special categories of personal data are subject to measures to ensure that the personal data processed are secured, protected, subject to suitable safeguards, including strict controls and documentation of the access, to avoid misuse and ensure that only authorised persons have access to those personal data with appropriate confidentiality obligations;

(d) the special categories of personal data are not to be transmitted, transferred or otherwise accessed by other parties;

(e) the special categories of personal data are deleted once the bias has been corrected or the personal data has reached the end of its retention period, whichever comes first;

(f) the records of processing activities pursuant to Regulations (EU) 2016/679 and (EU) 2018/1725 and Directive (EU) 2016/680 include the reasons why the processing of special categories of personal data was strictly necessary to detect and correct biases, and why that objective could not be achieved by processing other data.

6. For the development of high-risk AI systems not using techniques involving the training of AI models, paragraphs 2 to 5 apply only to the testing data sets.

Article 11

Technical documentation

1. The technical documentation of a high-risk AI system shall be drawn up before that system is placed on the market or put into service and shall be kept up-to date.

The technical documentation shall be drawn up in such a way as to demonstrate that the high-risk AI system complies with the requirements set out in this Section and to provide national competent authorities and notified bodies with the necessary information in a clear and comprehensive form to assess the compliance of the AI system with those requirements. It shall contain, at a minimum, the elements set out in Annex IV. SMEs, including start-ups, may provide the elements of the technical documentation specified in Annex IV in a simplified manner. To that end, the Commission shall establish a simplified technical documentation form targeted at the needs of small and microenterprises. Where an SME, including a start-up, opts to provide the information required in Annex IV in a simplified manner, it shall use the form referred to in this paragraph. Notified bodies shall accept the form for the purposes of the conformity assessment.

2. Where a high-risk AI system related to a product covered by the Union harmonisation legislation listed in Section A of Annex I is placed on the market or put into service, a single set of technical documentation shall be drawn up containing all the information set out in paragraph 1, as well as the information required under those legal acts.

3. The Commission is empowered to adopt delegated acts in accordance with Article 97 in order to amend Annex IV, where necessary, to ensure that, in light of technical progress, the technical documentation provides all the information necessary to assess the compliance of the system with the requirements set out in this Section.

5. 在严格必要的情况下，为根据本条第(2)款第(f)项和第(g)项确保与高风险人工智能系统相关的偏见检测和纠正之目的，此类系统的提供者可例外处理特殊类别的个人数据，但须对自然人的基本权利和自由采取适当保障措施。除条例(EU) 2016/679和(EU) 2018/1725以及指令(EU) 2016/680所规定的条款外，为进行此类处理，还必须满足以下所有条件：

(a) 偏见检测和纠正无法通过处理其他数据(包括合成数据或匿名化数据)有效实现；

(b) 特殊类别的个人数据在个人数据的再利用方面受到技术限制，并受到最先进的安全和隐私保护措施(包括假名化)的约束；

(c) 特殊类别的个人数据受到措施约束，以确保所处理的个人数据得到保护、保障，并受到适当的安全防护，包括严格的访问控制和记录，以避免滥用并确保只有经授权的人员在适当的保密义务下才能访问这些个人数据；

(d) 特殊类别的个人数据不得由其他方传输、转移或以其他方式访问；

(e) 一旦偏见得到纠正或个人数据达到保留期限届满(以先到者为准)，特殊类别的个人数据即被删除；

(f) 根据条例(EU) 2016/679和(EU) 2018/1725以及指令(EU) 2016/680的处理活动记录应包括为何处理特殊类别的个人数据对于检测和纠正偏见是严格必要的，以及为何该目标无法通过处理其他数据来实现的原因。

6. 对于不使用涉及人工智能模型训练的技术开发的高风险人工智能系统，第2至第5段仅适用于测试数据集。

第11条

技术文档

1. 高风险人工智能系统的技术文档应在该系统投放市场或投入使用之前编制，并应保持最新。

技术文档的编制方式应能证明高风险人工智能系统符合本节规定的要求，并以清晰、全面的形式向国家主管机关和公告机构提供必要信息，以便评估人工智能系统对这些要求的符合性。技术文档至少应包含附件四所列要素。中小企业，包括初创企业，可以简化方式提供附件四规定的技术文档要素。为此，欧盟委员会应制定针对小型和微型企业需求的简化技术文档表格。当中小企业，包括初创企业，选择以简化方式提供附件四所要求的信息时，应使用本段所指的表格。公告机构为合格评定目的应接受该表格。

2. 当与附件I A节所列欧盟协调立法所涵盖的产品相关的高风险人工智能系统投放市场或投入使用，应编制一套单一的技术文档，其中包含第1段所列的所有信息以及这些法律法案所要求的信息。

3. 委员会被授权根据第97条通过授权法案，以便在必要时修订附件IV，以确保鉴于技术进步，技术文档提供评估系统是否符合本节所列要求所需的所有信息。

Article 12

Record-keeping

1. High-risk AI systems shall technically allow for the automatic recording of events (logs) over the lifetime of the system.

2. In order to ensure a level of traceability of the functioning of a high-risk AI system that is appropriate to the intended purpose of the system, logging capabilities shall enable the recording of events relevant for:

(a) identifying situations that may result in the high-risk AI system presenting a risk within the meaning of Article 79(1) or in a substantial modification;

(b) facilitating the post-market monitoring referred to in Article 72; and

(c) monitoring the operation of high-risk AI systems referred to in Article 26(5).

3. For high-risk AI systems referred to in point 1 (a), of Annex III, the logging capabilities shall provide, at a minimum:

(a) recording of the period of each use of the system (start date and time and end date and time of each use);

(b) the reference database against which input data has been checked by the system;

(c) the input data for which the search has led to a match;

(d) the identification of the natural persons involved in the verification of the results, as referred to in Article 14(5).

Article 13

Transparency and provision of information to deployers

1. High-risk AI systems shall be designed and developed in such a way as to ensure that their operation is sufficiently transparent to enable deployers to interpret a system's output and use it appropriately. An appropriate type and degree of transparency shall be ensured with a view to achieving compliance with the relevant obligations of the provider and deployer set out in Section 3.

2. High-risk AI systems shall be accompanied by instructions for use in an appropriate digital format or otherwise that include concise, complete, correct and clear information that is relevant, accessible and comprehensible to deployers.

3. The instructions for use shall contain at least the following information:

(a) the identity and the contact details of the provider and, where applicable, of its authorised representative;

(b) the characteristics, capabilities and limitations of performance of the high-risk AI system, including:

(i) its intended purpose;

(ii) the level of accuracy, including its metrics, robustness and cybersecurity referred to in Article 15 against which the high-risk AI system has been tested and validated and which can be expected, and any known and foreseeable circumstances that may have an impact on that expected level of accuracy, robustness and cybersecurity;

(iii) any known or foreseeable circumstance, related to the use of the high-risk AI system in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may lead to risks to the health and safety or fundamental rights referred to in Article 9(2);

(iv) where applicable, the technical capabilities and characteristics of the high-risk AI system to provide information that is relevant to explain its output;

第12条

记录保存

1. 高风险人工智能系统应在技术上允许在系统生命周期内自动记录事件(日志)。

2. 为确保高风险人工智能系统运行的可追溯性水平适合系统的预期目的，日志记录能力应能够记录与以下相关的事件：

(a) 识别可能导致高风险人工智能系统呈现第79(1)条含义内的风险或导致实质性修改的情况；

(b) 便利第72条所指的市场后监测；以及

(c) 监测第26(5)条所述高风险AI系统的运行情况。

3. 对于附件III第1(a)点所述的高风险人工智能系统，日志记录能力应至少提供：

(a) 记录系统每次使用的时段(每次使用的开始日期和时间以及结束日期和时间)；

(b) 系统已对照检查输入数据的参考数据库；

(c) 搜索已匹配到的输入数据；

(d) 识别参与结果验证的自然人，如第14(5)条所述。

第13条

透明度和向部署者提供信息

1. 高风险人工智能系统的设计和开发应确保其运行具有足够的透明度，使部署者能够解释系统的输出并适当使用。应确保适当类型和程度的透明度，以实现遵守第3节所列提供者和部署者的相关义务。

2. 高风险人工智能系统应附有以适当的数字格式或其他格式提供的使用说明，其中包含对部署者相关、可访问和可理解的简明、完整、正确和清晰的信息。

3. 使用说明应至少包含以下信息：

(a) 提供者的身份和联系方式，以及适用时其授权代表的身份和联系方式；

(b) 高风险人工智能系统的性能特征、能力和局限性，包括：

(i) 其预期用途；

(ii) 第15条所述准确度水平(包括其指标)、稳健性和网络安全水平，高风险人工智能系统已针对该水平进行测试和验证且可预期达到该水平，以及任何可能对该预期准确度、稳健性和网络安全水平产生影响的已知和可预见情况；

(iii) 与按照其预期目的或在合理可预见的误用条件下使用高风险人工智能系统有关的任何已知或可预见的情况，该情况可能导致第9(2)条所述的对健康和安全或基本权利的风险；

(iv) 在适用的情况下，高风险人工智能系统提供与解释其输出相关的信息的技术能力和特性；

(v) when appropriate, its performance regarding specific persons or groups of persons on which the system is intended to be used;

(vi) when appropriate, specifications for the input data, or any other relevant information in terms of the training, validation and testing data sets used, taking into account the intended purpose of the high-risk AI system;

(vii) where applicable, information to enable deployers to interpret the output of the high-risk AI system and use it appropriately;

(c) the changes to the high-risk AI system and its performance which have been pre-determined by the provider at the moment of the initial conformity assessment, if any;

(d) the human oversight measures referred to in Article 14, including the technical measures put in place to facilitate the interpretation of the outputs of the high-risk AI systems by the deployers;

(e) the computational and hardware resources needed, the expected lifetime of the high-risk AI system and any necessary maintenance and care measures, including their frequency, to ensure the proper functioning of that AI system, including as regards software updates;

(f) where relevant, a description of the mechanisms included within the high-risk AI system that allows deployers to properly collect, store and interpret the logs in accordance with Article 12.

Article 14

Human oversight

1. High-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which they are in use.

2. Human oversight shall aim to prevent or minimise the risks to health, safety or fundamental rights that may emerge when a high-risk AI system is used in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, in particular where such risks persist despite the application of other requirements set out in this Section.

3. The oversight measures shall be commensurate with the risks, level of autonomy and context of use of the high-risk AI system, and shall be ensured through either one or both of the following types of measures:

(a) measures identified and built, when technically feasible, into the high-risk AI system by the provider before it is placed on the market or put into service;

(b) measures identified by the provider before placing the high-risk AI system on the market or putting it into service and that are appropriate to be implemented by the deployer.

4. For the purpose of implementing paragraphs 1, 2 and 3, the high-risk AI system shall be provided to the deployer in such a way that natural persons to whom human oversight is assigned are enabled, as appropriate and proportionate:

(a) to properly understand the relevant capacities and limitations of the high-risk AI system and be able to duly monitor its operation, including in view of detecting and addressing anomalies, dysfunctions and unexpected performance;

(b) to remain aware of the possible tendency of automatically relying or over-relying on the output produced by a high-risk AI system (automation bias), in particular for high-risk AI systems used to provide information or recommendations for decisions to be taken by natural persons;

(c) to correctly interpret the high-risk AI system's output, taking into account, for example, the interpretation tools and methods available;

(v) 在适当的情况下，其针对系统预期使用所针对的特定人员或人群的性能；

(vi) 在适当的情况下，输入数据的规格，或所使用的训练、验证和测试数据集方面的任何其他相关信息，同时考虑高风险人工智能系统的预期目的；

(vii) 在适用的情况下，使部署者能够解释高风险人工智能系统的输出并适当使用该输出的信息；

(c) 提供者在初始合格评定之时预先确定的高风险人工智能系统及其性能的变更(如有);

(d) 第14条所述的人类监督措施，包括为便于部署者解释高风险人工智能系统的输出而采取的技术措施；

(e) 所需计算和硬件资源、高风险人工智能系统的预期使用寿命以及任何必要的维护和保养措施(包括其频率)，以确保该人工智能系统的正常运行，包括在软件更新方面；

(f) 在相关的情况下，对高风险人工智能系统中所包含的机制的描述，该机制允许部署者按照第12条正确收集、存储和解释日志。

第14条

人工监督

1. 高风险人工智能系统的设计和开发方式，包括配备适当的人机界面工具，应使其在使用期间能够被自然人员有效监督。

2. 人类监督应旨在防止或尽量减少高风险人工智能系统按照其预期目的使用或在合理可预见的误用条件下使用时可能出现的对健康、安全或基本权利的风险，特别是在尽管适用了本节规定的其他要求但此类风险仍然存在的情况下。

3. 监督措施应与高风险人工智能系统的风险、自主程度和使用情境相称，并应通过以下两类措施中的一类或两类予以确保：

(a) 由提供者在高风险人工智能系统投放市场或投入使用之前，在技术可行的情况下识别并内置于该系统中的措施；

(b) 由提供者在将高风险人工智能系统投放市场或投入使用之前识别、且适合由部署者实施的措施。

4. 为实施第1款、第2款和第3款，高风险人工智能系统向部署者提供的方式应使被指派进行人类监督的自然人员能够在适当且相称的情况下：

(a) 正确理解高风险人工智能系统的相关能力和局限性，并能够适当监测其运行，包括发现和处理异常、故障和意外性能；

(b) 始终意识到可能倾向于自动依赖或过度依赖高风险人工智能系统产生的输出(自动化偏见)，特别是对于用于为自然人员待作出的决策提供信息或建议的高风险人工智能系统；

(c) 正确解释高风险人工智能系统的输出，同时考虑到例如可用的解释工具和方法；

(d) to decide, in any particular situation, not to use the high-risk AI system or to otherwise disregard, override or reverse the output of the high-risk AI system;

(e) to intervene in the operation of the high-risk AI system or interrupt the system through a 'stop' button or a similar procedure that allows the system to come to a halt in a safe state.

5. For high-risk AI systems referred to in point 1(a) of Annex III, the measures referred to in paragraph 3 of this Article shall be such as to ensure that, in addition, no action or decision is taken by the deployer on the basis of the identification resulting from the system unless that identification has been separately verified and confirmed by at least two natural persons with the necessary competence, training and authority.

The requirement for a separate verification by at least two natural persons shall not apply to high-risk AI systems used for the purposes of law enforcement, migration, border control or asylum, where Union or national law considers the application of this requirement to be disproportionate.

Article 15

Accuracy, robustness and cybersecurity

1. High-risk AI systems shall be designed and developed in such a way that they achieve an appropriate level of accuracy, robustness, and cybersecurity, and that they perform consistently in those respects throughout their lifecycle.

2. To address the technical aspects of how to measure the appropriate levels of accuracy and robustness set out in paragraph 1 and any other relevant performance metrics, the Commission shall, in cooperation with relevant stakeholders and organisations such as metrology and benchmarking authorities, encourage, as appropriate, the development of benchmarks and measurement methodologies.

3. The levels of accuracy and the relevant accuracy metrics of high-risk AI systems shall be declared in the accompanying instructions of use.

4. High-risk AI systems shall be as resilient as possible regarding errors, faults or inconsistencies that may occur within the system or the environment in which the system operates, in particular due to their interaction with natural persons or other systems. Technical and organisational measures shall be taken in this regard.

The robustness of high-risk AI systems may be achieved through technical redundancy solutions, which may include backup or fail-safe plans.

High-risk AI systems that continue to learn after being placed on the market or put into service shall be developed in such a way as to eliminate or reduce as far as possible the risk of possibly biased outputs influencing input for future operations (feedback loops), and as to ensure that any such feedback loops are duly addressed with appropriate mitigation measures.

5. High-risk AI systems shall be resilient against attempts by unauthorised third parties to alter their use, outputs or performance by exploiting system vulnerabilities.

The technical solutions aiming to ensure the cybersecurity of high-risk AI systems shall be appropriate to the relevant circumstances and the risks.

The technical solutions to address AI specific vulnerabilities shall include, where appropriate, measures to prevent, detect, respond to, resolve and control for attacks trying to manipulate the training data set (data poisoning), or pre-trained components used in training (model poisoning), inputs designed to cause the AI model to make a mistake (adversarial examples or model evasion), confidentiality attacks or model flaws.

(d) 在任何特定情况下决定不使用高风险人工智能系统，或以其他方式无视、推翻或逆转高风险人工智能系统的输出；

(e) 干预高风险人工智能系统的运行，或通过"停止"按钮或类似程序中断系统，使系统能够在安全状态下停止运行。

5. 对于附件三第1(a)点所述的高风险人工智能系统，本条第3款所述措施应确保，此外，部署者不得基于该系统所得出的识别结果采取任何行动或作出任何决定，除非该识别结果已由至少两名具备必要能力、培训和权限的自然人员单独核实和确认。

对于用于执法、移民、边境控制或庇护目的的高风险人工智能系统，如果联盟或国家法律认为适用该要求不相称，则至少两名自然人单独核实的要求不适用。

第15条

准确性、稳健性和网络安全

1. 高风险人工智能系统的设计和开发方式应使其达到适当的准确性、稳健性和网络安全水平，并在其整个生命周期内在这些方面保持一致的表现。

2. 为解决如何衡量第1款规定的适当准确性和稳健性水平以及任何其他相关性能指标的技术问题，委员会应与相关利益相关方和组织(如计量和基准测试机构)合作，酌情鼓励制定基准和测量方法。

3. 高风险人工智能系统的准确性水平和相关准确性指标应在随附的使用说明中予以声明。

4. 高风险人工智能系统应尽可能对系统内部或系统运行环境中可能出现的错误、故障或不一致具有韧性，特别是由于其与自然人员或其他系统的交互而产生的错误、故障或不一致。为此应采取技术和组织措施。

高风险人工智能系统的稳健性可通过技术冗余解决方案实现，其中可包括备份或故障安全计划。

在投放市场或投入使用后继续学习的高风险人工智能系统，其开发方式应尽可能消除或降低可能带有偏见的输出影响未来操作输入的风险(反馈回路)，并确保任何此类反馈回路均通过适当的缓解措施得到妥善处理。

5. 高风险人工智能系统应具有韧性，能够抵御未经授权的第三方利用系统脆弱性改变其使用、输出或性能的企图。

旨在确保高风险人工智能系统网络安全的技术解决方案应与相关情况和风险相适应。

应对人工智能特定脆弱性的技术解决方案应酌情包括预防、检测、响应、解决和控制以下攻击的措施：试图操纵训练数据集(数据投毒)或训练中使用的预训练组件(模型投毒)、旨在使人工智能模型出错的输入(对抗性样本或模型规避)、机密性攻击或模型缺陷。

SECTION 3

Obligations of providers and deployers of high-risk AI systems and other parties

Article 16

Obligations of providers of high-risk AI systems

Providers of high-risk AI systems shall:

(a) ensure that their high-risk AI systems are compliant with the requirements set out in Section 2;

(b) indicate on the high-risk AI system or, where that is not possible, on its packaging or its accompanying documentation, as applicable, their name, registered trade name or registered trade mark, the address at which they can be contacted;

(c) have a quality management system in place which complies with Article 17;

(d) keep the documentation referred to in Article 18;

(e) when under their control, keep the logs automatically generated by their high-risk AI systems as referred to in Article 19;

(f) ensure that the high-risk AI system undergoes the relevant conformity assessment procedure as referred to in Article 43, prior to its being placed on the market or put into service;

(g) draw up an EU declaration of conformity in accordance with Article 47;

(h) affix the CE marking to the high-risk AI system or, where that is not possible, on its packaging or its accompanying documentation, to indicate conformity with this Regulation, in accordance with Article 48;

(i) comply with the registration obligations referred to in Article 49(1);

(j) take the necessary corrective actions and provide information as required in Article 20;

(k) upon a reasoned request of a national competent authority, demonstrate the conformity of the high-risk AI system with the requirements set out in Section 2;

(l) ensure that the high-risk AI system complies with accessibility requirements in accordance with Directives (EU) 2016/2102 and (EU) 2019/882.

Article 17

Quality management system

1. Providers of high-risk AI systems shall put a quality management system in place that ensures compliance with this Regulation. That system shall be documented in a systematic and orderly manner in the form of written policies, procedures and instructions, and shall include at least the following aspects:

(a) a strategy for regulatory compliance, including compliance with conformity assessment procedures and procedures for the management of modifications to the high-risk AI system;

(b) techniques, procedures and systematic actions to be used for the design, design control and design verification of the high-risk AI system;

(c) techniques, procedures and systematic actions to be used for the development, quality control and quality assurance of the high-risk AI system;

(d) examination, test and validation procedures to be carried out before, during and after the development of the high-risk AI system, and the frequency with which they have to be carried out;

第3节

高风险人工智能系统提供者和部署者及其他方的义务

第16条

高风险人工智能系统提供者的义务

高风险人工智能系统的提供者应当：

(a) 确保其高风险人工智能系统符合第2节规定的要求；

(b) 在高风险人工智能系统上，或在无法做到的情况下在其包装或随附文件上(视情况而定)，标明其名称、注册商号或注册商标以及可联系到他们的地址；

(c) 建立符合第17条的质量管理体系；

(d) 保存第18条所述的文件；(e) 在其控制范围内，保存其高风险人工智能系统自动生成的第19条所述的日志；

(f) 确保高风险人工智能系统在投放市场或投入使用之前经过第43条所述的相关合格评定程序；

(g) 按照Article 47起草EU符合性声明；

(h) 在高风险人工智能系统上，或在无法做到的情况下在其包装或随附文件上，加贴CE 标志，以表明符合本法规，依照第48条；

(i) 遵守第49(1)条所述的登记义务；

(j) 采取必要的纠正措施并提供第20条所要求的信息；(k) 在国家主管机关提出合理请求时，证明高风险人工智能系统符合第2节规定的要求；

(l) 确保高风险人工智能系统符合Directives(EU) 2016/2102和(EU) 2019/882规定的无障碍要求。

第17条

质量管理体系

1. 高风险人工智能系统的提供者应建立质量管理体系，以确保符合本法规。该体系应以书面政策、程序和指令的形式，以系统和有序的方式记录，并应至少包括以下方面：

(a) 法规合规策略，包括遵守合格评定程序以及高风险人工智能系统修改管理程序；

(b) 用于高风险人工智能系统设计、设计控制和设计验证的技术、程序和系统性行动；

(c) 用于高风险人工智能系统开发、质量控制和质量保证的技术、程序和系统性行动；

(d) 在高风险人工智能系统开发之前、期间和之后应进行的检查、测试和验证程序，以及必须进行这些程序的频率；

(e) technical specifications, including standards, to be applied and, where the relevant harmonised standards are not applied in full or do not cover all of the relevant requirements set out in Section 2, the means to be used to ensure that the high-risk AI system complies with those requirements;

(f) systems and procedures for data management, including data acquisition, data collection, data analysis, data labelling, data storage, data filtration, data mining, data aggregation, data retention and any other operation regarding the data that is performed before and for the purpose of the placing on the market or the putting into service of high-risk AI systems;

(g) the risk management system referred to in Article 9;

(h) the setting-up, implementation and maintenance of a post-market monitoring system, in accordance with Article 72;

(i) procedures related to the reporting of a serious incident in accordance with Article 73;

(j) the handling of communication with national competent authorities, other relevant authorities, including those providing or supporting the access to data, notified bodies, other operators, customers or other interested parties;

(k) systems and procedures for record-keeping of all relevant documentation and information;

(l) resource management, including security-of-supply related measures;

(m) an accountability framework setting out the responsibilities of the management and other staff with regard to all the aspects listed in this paragraph.

2. The implementation of the aspects referred to in paragraph 1 shall be proportionate to the size of the provider's organisation. Providers shall, in any event, respect the degree of rigour and the level of protection required to ensure the compliance of their high-risk AI systems with this Regulation.

3. Providers of high-risk AI systems that are subject to obligations regarding quality management systems or an equivalent function under relevant sectoral Union law may include the aspects listed in paragraph 1 as part of the quality management systems pursuant to that law.

4. For providers that are financial institutions subject to requirements regarding their internal governance, arrangements or processes under Union financial services law, the obligation to put in place a quality management system, with the exception of paragraph 1, points (g), (h) and (i) of this Article, shall be deemed to be fulfilled by complying with the rules on internal governance arrangements or processes pursuant to the relevant Union financial services law. To that end, any harmonised standards referred to in Article 40 shall be taken into account.

Article 18

Documentation keeping

1. The provider shall, for a period ending 10 years after the high-risk AI system has been placed on the market or put into service, keep at the disposal of the national competent authorities:

(a) the technical documentation referred to in Article 11;

(b) the documentation concerning the quality management system referred to in Article 17;

(c) the documentation concerning the changes approved by notified bodies, where applicable;

(d) the decisions and other documents issued by the notified bodies, where applicable;

(e) the EU declaration of conformity referred to in Article 47.

(e) 拟适用的技术规范，包括标准，以及在相关协调标准未完全适用或未涵盖第2节所列全部相关要求时，为确保高风险人工智能系统符合这些要求而采用的方法；

(f) 数据管理系统和程序，包括数据获取、数据收集、数据分析、数据标注、数据存储、数据过滤、数据挖掘、数据聚合、数据保留以及在投放市场或投入使用高风险人工智能系统之前和为此目的对数据进行的任何其他操作；

(g) 第9条所指的风险管理系统；

(h) 根据第72条，建立、实施和维护上市后监测系统；

(i) 依照第73条报告严重事件的相关程序；

(j) 处理与国家主管机关、其他相关机关(包括提供或支持数据访问的机关)、公告机构、其他运营者、客户或其他利益相关方的沟通；

(k) 保存所有相关文档和信息的记录系统和程序；

(l) 资源管理，包括与供应安全相关的措施；

(m) 一个问责框架，规定管理层和其他工作人员对本段所列所有方面的责任。

2. 第1款所述各方面的实施应与提供者组织的规模成比例。提供者在任何情况下均应遵守确保其高风险人工智能系统符合本条例所需的严格程度和保护水平。

3. 受相关联盟部门法下质量管理体系或同等职能义务约束的高风险人工智能系统提供者，可将第1款所列各方面作为依照该法建立的质量管理体系的一部分。

4. 对于作为金融机构且须遵守欧盟金融服务法下有关其内部治理、安排或流程要求的提供者，通过遵守相关欧盟金融服务法关于内部治理安排或流程的规则，即应视为已履行建立质量管理体系的义务，但本条第1款(g)、(h)和(i)项除外。为此，应考虑第40条提及的任何协调标准。

第18条

文件保存

1. 提供者应在高风险人工智能系统投放市场或投入使用后10年期限届满前，将以下内容供国家主管机关查阅：

(a) 第11条所指的技术文档；

(b) 第17条所述质量管理体系的相关文档；

(c) 适用时，公告机构批准的变更的相关文档；

(d) 公告机构作出的决定和其他文件(如适用)；

(e) 第47条所指的欧盟符合性声明。

2. Each Member State shall determine conditions under which the documentation referred to in paragraph 1 remains at the disposal of the national competent authorities for the period indicated in that paragraph for the cases when a provider or its authorised representative established on its territory goes bankrupt or ceases its activity prior to the end of that period.

3. Providers that are financial institutions subject to requirements regarding their internal governance, arrangements or processes under Union financial services law shall maintain the technical documentation as part of the documentation kept under the relevant Union financial services law.

Article 19

Automatically generated logs

1. Providers of high-risk AI systems shall keep the logs referred to in Article 12(1), automatically generated by their high-risk AI systems, to the extent such logs are under their control. Without prejudice to applicable Union or national law, the logs shall be kept for a period appropriate to the intended purpose of the high-risk AI system, of at least six months, unless provided otherwise in the applicable Union or national law, in particular in Union law on the protection of personal data.

2. Providers that are financial institutions subject to requirements regarding their internal governance, arrangements or processes under Union financial services law shall maintain the logs automatically generated by their high-risk AI systems as part of the documentation kept under the relevant financial services law.

Article 20

Corrective actions and duty of information

1. Providers of high-risk AI systems which consider or have reason to consider that a high-risk AI system that they have placed on the market or put into service is not in conformity with this Regulation shall immediately take the necessary corrective actions to bring that system into conformity, to withdraw it, to disable it, or to recall it, as appropriate. They shall inform the distributors of the high-risk AI system concerned and, where applicable, the deployers, the authorised representative and importers accordingly.

2. Where the high-risk AI system presents a risk within the meaning of Article 79(1) and the provider becomes aware of that risk, it shall immediately investigate the causes, in collaboration with the reporting deployer, where applicable, and inform the market surveillance authorities competent for the high-risk AI system concerned and, where applicable, the notified body that issued a certificate for that high-risk AI system in accordance with Article 44, in particular, of the nature of the non-compliance and of any relevant corrective action taken.

Article 21

Cooperation with competent authorities

1. Providers of high-risk AI systems shall, upon a reasoned request by a competent authority, provide that authority all the information and documentation necessary to demonstrate the conformity of the high-risk AI system with the requirements set out in Section 2, in a language which can be easily understood by the authority in one of the official languages of the institutions of the Union as indicated by the Member State concerned.

2. Upon a reasoned request by a competent authority, providers shall also give the requesting competent authority, as applicable, access to the automatically generated logs of the high-risk AI system referred to in Article 12(1), to the extent such logs are under their control.

3. Any information obtained by a competent authority pursuant to this Article shall be treated in accordance with the confidentiality obligations set out in Article 78.

2. 各成员国应确定在提供者或其设立在其领土上的授权代表在该期限结束前破产或停止活动的情况下，第1款所述文档在该款所指期限内继续供国家主管机关查阅的条件。

3. 属于金融机构且受联盟金融服务法下内部治理、安排或程序要求约束的提供者，应作为依照相关联盟金融服务法保存的文档的一部分，保存技术文档。

第19条

自动生成的日志

1. 高风险人工智能系统的提供者应保存第12(1)条提及的、由其高风险人工智能系统自动生成的日志，但以该等日志在其控制范围内为限。在不影响适用的欧盟法或国内法的情况下，日志的保存期限应与高风险人工智能系统的预期目的相适应，且至少为六个月，除非适用的欧盟法或国内法，特别是欧盟关于个人数据保护的法律另有规定。

2. 属于金融机构且受联盟金融服务法下内部治理、安排或程序要求约束的提供者，应作为依照相关金融服务法保存的文档的一部分，保存其高风险人工智能系统自动生成的日志。

第20条

纠正措施和信息义务

1. 高风险人工智能系统的提供者如认为或有理由认为其已投放市场或投入使用的高风险人工智能系统不符合本条例，应立即采取必要的纠正措施使该系统符合要求、将其撤出市场、将其停用或酌情将其召回。提供者应相应通知相关高风险人工智能系统的分销商，并在适用情况下通知部署者、授权代表和进口商。

2. 如高风险人工智能系统存在第79(1)条含义范围内的风险，且提供者知悉该风险，提供者应立即调查原因，并在适用情况下与进行报告的部署者合作，通知对相关高风险人工智能系统具有管辖权的市场监督机构，并在适用情况下通知根据第44条为该高风险人工智能系统颁发证书的公告机构，尤其应通知不符合的性质以及所采取的任何相关纠正措施。

第21条

与主管机关的合作

1. 高风险人工智能系统的提供者应当在主管机关提出合理请求时，以该机关能够轻松理解的语言、以相关成员国指明的欧盟机构官方语言之一，向该机关提供证明该高风险人工智能系统符合第2节规定要求所需的所有信息和文档。

2. 在主管机关提出合理请求时，提供者还应酌情向提出请求的主管机关提供第12条第1款所述高风险人工智能系统自动生成的日志的访问权限，前提是此类日志在其控制之下。

3. 主管机关依照本条获得的任何信息，均应按照第78条规定的保密义务处理。

Article 22

Authorised representatives of providers of high-risk AI systems

1. Prior to making their high-risk AI systems available on the Union market, providers established in third countries shall, by written mandate, appoint an authorised representative which is established in the Union.

2. The provider shall enable its authorised representative to perform the tasks specified in the mandate received from the provider.

3. The authorised representative shall perform the tasks specified in the mandate received from the provider. It shall provide a copy of the mandate to the market surveillance authorities upon request, in one of the official languages of the institutions of the Union, as indicated by the competent authority. For the purposes of this Regulation, the mandate shall empower the authorised representative to carry out the following tasks:

(a) verify that the EU declaration of conformity referred to in Article 47 and the technical documentation referred to in Article 11 have been drawn up and that an appropriate conformity assessment procedure has been carried out by the provider;

(b) keep at the disposal of the competent authorities and national authorities or bodies referred to in Article 74(10), for a period of 10 years after the high-risk AI system has been placed on the market or put into service, the contact details of the provider that appointed the authorised representative, a copy of the EU declaration of conformity referred to in Article 47, the technical documentation and, if applicable, the certificate issued by the notified body;

(c) provide a competent authority, upon a reasoned request, with all the information and documentation, including that referred to in point (b) of this subparagraph, necessary to demonstrate the conformity of a high-risk AI system with the requirements set out in Section 2, including access to the logs, as referred to in Article 12(1), automatically generated by the high-risk AI system, to the extent such logs are under the control of the provider;

(d) cooperate with competent authorities, upon a reasoned request, in any action the latter take in relation to the high-risk AI system, in particular to reduce and mitigate the risks posed by the high-risk AI system;

(e) where applicable, comply with the registration obligations referred to in Article 49(1), or, if the registration is carried out by the provider itself, ensure that the information referred to in point 3 of Section A of Annex VIII is correct.

The mandate shall empower the authorised representative to be addressed, in addition to or instead of the provider, by the competent authorities, on all issues related to ensuring compliance with this Regulation.

4. The authorised representative shall terminate the mandate if it considers or has reason to consider the provider to be acting contrary to its obligations pursuant to this Regulation. In such a case, it shall immediately inform the relevant market surveillance authority, as well as, where applicable, the relevant notified body, about the termination of the mandate and the reasons therefor.

Article 23

Obligations of importers

1. Before placing a high-risk AI system on the market, importers shall ensure that the system is in conformity with this Regulation by verifying that:

(a) the relevant conformity assessment procedure referred to in Article 43 has been carried out by the provider of the high-risk AI system;

(b) the provider has drawn up the technical documentation in accordance with Article 11 and Annex IV;

(c) the system bears the required CE marking and is accompanied by the EU declaration of conformity referred to in Article 47 and instructions for use;

(d) the provider has appointed an authorised representative in accordance with Article 22(1).

第22条

高风险人工智能系统提供者的授权代表

1. 在将其高风险人工智能系统投放欧盟市场之前，设立在第三国的提供者应通过书面授权，指定一名设立在欧盟的授权代表。

2. 提供者应使其授权代表能够执行提供者所授予授权中规定的任务。

3. 授权代表应执行提供者所授予授权中规定的任务。应市场监督机构的要求，授权代表应以欧盟机构官方语言之一提供授权副本，具体语言由主管机关指定。为本条例之目的，授权应赋予授权代表执行以下任务：

(a) 核实第47条所述欧盟符合性声明和第11条所述技术文档已经起草，并且提供者已经执行了适当的合格评定程序；

(b) 在高风险人工智能系统投放市场或投入使用后10年内，向主管机关和第74(10)条所述国家主管机关或机构提供指定授权代表的提供者的联系方式、第47条所述欧盟符合性声明的副本、技术文档以及(如适用)公告机构签发的证书；

(c) 应合理请求，向主管机关提供所有必要的信息和文档，包括本项(b)点所述的信息和文档，以证明高风险人工智能系统符合第2节规定的要求，包括在提供者控制范围内访问高风险人工智能系统自动生成的、第12(1)条所述日志；

(d) 应合理请求，与主管机关合作，配合其就高风险人工智能系统采取的任何行动，特别是减少和缓解高风险人工智能系统所构成的风险；

(e) 在适用情况下，遵守第49(1)条所述注册义务，或者，如果注册由提供者自行进行，确保附件VIII第A节第3点所述信息正确。

的行为违反其依据本条例承担的义务，应终止授权。在此情况下，其应立即通知相关市场监督机构以及(如适用)相关公告机构，说明授权的终止及终止原因。

4. 授权代表如认为或有理由认为提供者违反本条例规定的义务，应终止授权。在此情况下，授权代表应立即通知相关市场监督机构以及(如适用)相关公告机构，说明授权终止及其原因。

第23条

进口商的义务

1. 在将高风险人工智能系统投放市场之前，进口商应通过核实以下事项，确保该系统符合本条例：

(a) 高风险人工智能系统的提供者已执行第43条所述相关合格评定程序；

(b) 提供者已按照第11条和附件IV起草技术文档；

(c) 系统带有要求的CE 标志，并附有第47条所述欧盟符合性声明和使用说明；

(d) 提供者已按照第22(1)条指定授权代表。

2. Where an importer has sufficient reason to consider that a high-risk AI system is not in conformity with this Regulation, or is falsified, or accompanied by falsified documentation, it shall not place the system on the market until it has been brought into conformity. Where the high-risk AI system presents a risk within the meaning of Article 79(1), the importer shall inform the provider of the system, the authorised representative and the market surveillance authorities to that effect.

3. Importers shall indicate their name, registered trade name or registered trade mark, and the address at which they can be contacted on the high-risk AI system and on its packaging or its accompanying documentation, where applicable.

4. Importers shall ensure that, while a high-risk AI system is under their responsibility, storage or transport conditions, where applicable, do not jeopardise its compliance with the requirements set out in Section 2.

5. Importers shall keep, for a period of 10 years after the high-risk AI system has been placed on the market or put into service, a copy of the certificate issued by the notified body, where applicable, of the instructions for use, and of the EU declaration of conformity referred to in Article 47.

6. Importers shall provide the relevant competent authorities, upon a reasoned request, with all the necessary information and documentation, including that referred to in paragraph 5, to demonstrate the conformity of a high-risk AI system with the requirements set out in Section 2 in a language which can be easily understood by them. For this purpose, they shall also ensure that the technical documentation can be made available to those authorities.

7. Importers shall cooperate with the relevant competent authorities in any action those authorities take in relation to a high-risk AI system placed on the market by the importers, in particular to reduce and mitigate the risks posed by it.

Article 24

Obligations of distributors

1. Before making a high-risk AI system available on the market, distributors shall verify that it bears the required CE marking, that it is accompanied by a copy of the EU declaration of conformity referred to in Article 47 and instructions for use, and that the provider and the importer of that system, as applicable, have complied with their respective obligations as laid down in Article 16, points (b) and (c) and Article 23(3).

2. Where a distributor considers or has reason to consider, on the basis of the information in its possession, that a high-risk AI system is not in conformity with the requirements set out in Section 2, it shall not make the high-risk AI system available on the market until the system has been brought into conformity with those requirements. Furthermore, where the high-risk AI system presents a risk within the meaning of Article 79(1), the distributor shall inform the provider or the importer of the system, as applicable, to that effect.

3. Distributors shall ensure that, while a high-risk AI system is under their responsibility, storage or transport conditions, where applicable, do not jeopardise the compliance of the system with the requirements set out in Section 2.

4. A distributor that considers or has reason to consider, on the basis of the information in its possession, a high-risk AI system which it has made available on the market not to be in conformity with the requirements set out in Section 2, shall take the corrective actions necessary to bring that system into conformity with those requirements, to withdraw it or recall it, or shall ensure that the provider, the importer or any relevant operator, as appropriate, takes those corrective actions. Where the high-risk AI system presents a risk within the meaning of Article 79(1), the distributor shall immediately inform the provider or importer of the system and the authorities competent for the high-risk AI system concerned, giving details, in particular, of the non-compliance and of any corrective actions taken.

5. Upon a reasoned request from a relevant competent authority, distributors of a high-risk AI system shall provide that authority with all the information and documentation regarding their actions pursuant to paragraphs 1 to 4 necessary to demonstrate the conformity of that system with the requirements set out in Section 2.

6. Distributors shall cooperate with the relevant competent authorities in any action those authorities take in relation to a high-risk AI system made available on the market by the distributors, in particular to reduce or mitigate the risk posed by it.

2. 进口商如有充分理由认为高风险人工智能系统不符合本条例，或系伪造，或附有伪造文档，则不得将该系统投放市场，直至其符合规定。如高风险人工智能系统存在第79(1)条含义范围内的风险，进口商应就此通知系统提供者、授权代表和市场监督机构。

3. 进口商应在高风险人工智能系统及其包装或随附文档(如适用)上标明其名称、注册商号或注册商标以及可联系地址。

4. 进口商应确保，在高风险人工智能系统由其负责期间，存储或运输条件(如适用)不会危及该系统符合第2节规定的要求。

5. 进口商应在高风险人工智能系统投放市场或投入使用后10年内，保存公告机构签发的证书(如适用)、使用说明以及第47条所述欧盟符合性声明的副本。

6. 进口商应应合理请求，以易于其理解的语言向相关主管机关提供所有必要的信息和文档，包括第5段所述的信息和文档，以证明高风险人工智能系统符合第2节规定的要求。为此，进口商还应确保能够向这些机关提供技术文档。

7. 进口商应与相关主管机关合作，配合其就进口商投放市场的高风险人工智能系统采取的任何行动，特别是减少和缓解该系统所构成的风险。

第24条

分销商的义务

1. 在将高风险人工智能系统投放市场之前，分销商应核实该系统带有要求的CE 标志，附有第47条所述欧盟符合性声明的副本和使用说明，并且该系统的提供者和进口商(如适用)已遵守第16条(b)点和(c)点以及第23(3)条规定的各自义务。

2. 分销商如根据其掌握的信息认为或有理由认为高风险人工智能系统不符合第2节规定的要求，则在该系统符合这些要求之前，不得将该高风险人工智能系统投放市场。此外，如该高风险人工智能系统存在第79(1)条意义上的风险，分销商应就此告知该系统的提供者或进口商(视情况而定)。

3. 分销商应确保，在高风险人工智能系统由其负责期间，存储或运输条件(如适用)不会危及该系统符合第2节规定的要求。

4. 分销商如根据其掌握的信息认为或有理由认为其已投放市场的高风险人工智能系统不符合第2节规定的要求，应采取必要的纠正措施使该系统符合这些要求、将其撤出市场或召回，或应确保提供者、进口商或任何相关运营者(视情况而定)采取这些纠正措施。如该高风险人工智能系统存在第79(1)条意义上的风险，分销商应立即告知该系统的提供者或进口商以及相关高风险人工智能系统的主管机构，尤其应详细说明不合规情况及所采取的任何纠正措施。

5. 应相关主管机关的合理请求，高风险人工智能系统的分销商应向该机关提供有关其根据第1至4段所采取行动的所有信息和文档，以证明该系统符合第2节规定的要求。

6. 分销商应与相关主管机关合作，配合其就分销商投放市场的高风险人工智能系统采取的任何行动，特别是减少或缓解该系统所构成的风险
它。

Article 25

Responsibilities along the AI value chain

1. Any distributor, importer, deployer or other third-party shall be considered to be a provider of a high-risk AI system for the purposes of this Regulation and shall be subject to the obligations of the provider under Article 16, in any of the following circumstances:

(a) they put their name or trademark on a high-risk AI system already placed on the market or put into service, without prejudice to contractual arrangements stipulating that the obligations are otherwise allocated;

(b) they make a substantial modification to a high-risk AI system that has already been placed on the market or has already been put into service in such a way that it remains a high-risk AI system pursuant to Article 6;

(c) they modify the intended purpose of an AI system, including a general-purpose AI system, which has not been classified as high-risk and has already been placed on the market or put into service in such a way that the AI system concerned becomes a high-risk AI system in accordance with Article 6.

2. Where the circumstances referred to in paragraph 1 occur, the provider that initially placed the AI system on the market or put it into service shall no longer be considered to be a provider of that specific AI system for the purposes of this Regulation. That initial provider shall closely cooperate with new providers and shall make available the necessary information and provide the reasonably expected technical access and other assistance that are required for the fulfilment of the obligations set out in this Regulation, in particular regarding the compliance with the conformity assessment of high-risk AI systems. This paragraph shall not apply in cases where the initial provider has clearly specified that its AI system is not to be changed into a high-risk AI system and therefore does not fall under the obligation to hand over the documentation.

3. In the case of high-risk AI systems that are safety components of products covered by the Union harmonisation legislation listed in Section A of Annex I, the product manufacturer shall be considered to be the provider of the high-risk AI system, and shall be subject to the obligations under Article 16 under either of the following circumstances:

(a) the high-risk AI system is placed on the market together with the product under the name or trademark of the product manufacturer;

(b) the high-risk AI system is put into service under the name or trademark of the product manufacturer after the product has been placed on the market.

4. The provider of a high-risk AI system and the third party that supplies an AI system, tools, services, components, or processes that are used or integrated in a high-risk AI system shall, by written agreement, specify the necessary information, capabilities, technical access and other assistance based on the generally acknowledged state of the art, in order to enable the provider of the high-risk AI system to fully comply with the obligations set out in this Regulation. This paragraph shall not apply to third parties making accessible to the public tools, services, processes, or components, other than general-purpose AI models, under a free and open-source licence.

The AI Office may develop and recommend voluntary model terms for contracts between providers of high-risk AI systems and third parties that supply tools, services, components or processes that are used for or integrated into high-risk AI systems. When developing those voluntary model terms, the AI Office shall take into account possible contractual requirements applicable in specific sectors or business cases. The voluntary model terms shall be published and be available free of charge in an easily usable electronic format.

5. Paragraphs 2 and 3 are without prejudice to the need to observe and protect intellectual property rights, confidential business information and trade secrets in accordance with Union and national law.

Article 26

Obligations of deployers of high-risk AI systems

1. Deployers of high-risk AI systems shall take appropriate technical and organisational measures to ensure they use such systems in accordance with the instructions for use accompanying the systems, pursuant to paragraphs 3 and 6.

第25条

人工智能价值链上的责任

1. 在以下任一情况下，任何分销商、进口商、部署者或其他第三方应被视为本条例意义上的高风险人工智能系统提供者，并应遵守第16条规定的提供者义务：

(a) 其在已投放市场或已投入使用的高风险人工智能系统上使用自己的名称或商标，但不影响约定以其他方式分配义务的合同安排；

(b) 其对已投放市场或已投入使用的高风险人工智能系统进行实质性修改，使其根据第6条仍为高风险人工智能系统；

(c) 其修改未被归类为高风险且已投放市场或已投入使用的人工智能系统(包括通用人工智能系统)的预期用途，使相关人工智能系统根据第6条成为高风险人工智能系统。

2. 如发生第1款所述情形，最初将人工智能系统投放市场或投入使用的提供者，就本条例而言不再被视为该特定人工智能系统的提供者。该原提供者应与新提供者密切合作，提供必要信息，并提供履行本条例规定义务所需的合理预期的技术访问和其他协助，特别是关于高风险人工智能系统合格评定合规方面的协助。如原提供者已明确说明其人工智能系统不得被改变为高风险人工智能系统，因而无义务移交文档，则本款不适用。

3. 对于属于附件I第A节所列欧盟协调立法所涵盖产品安全组件的高风险人工智能系统，在以下任一情况下，产品制造商应被视为该高风险人工智能系统的提供者，并应遵守第16条规定的义务：

(a) 高风险人工智能系统以产品制造商的名称或商标与产品一起投放市场；

(b) 高风险人工智能系统在产品投放市场后，以产品制造商的名称或商标投入使用。

4. 高风险人工智能系统的提供者与提供用于或集成于高风险人工智能系统的人工智能系统、工具、服务、组件或流程的第三方，应通过书面协议，基于公认的最新技术水平，明确必要的信息、能力、技术访问和其他协助，以使高风险人工智能系统的提供者能够完全遵守本条例规定的义务。本款不适用于以免费和开源许可证向公众提供工具、服务、流程或组件(通用人工智能模型除外)的第三方。

人工智能办公室可制定并推荐用于高风险人工智能系统提供者与供应高风险人工智能系统所用或集成于其中的工具、服务、组件或流程的第三方之间合同的自愿示范条款。在制定这些自愿示范条款时，人工智能办公室应考虑特定行业或业务情形中可能适用的合同要求。自愿示范条款应以易于使用的电子格式发布并免费提供。

5. 第2款和第3款不影响依照欧盟法和国家法尊重和保护知识产权、保密商业信息和商业秘密的需要。

第26条

高风险人工智能系统部署者的义务

1. 高风险人工智能系统的部署者应采取适当的技术和组织措施，确保其依照系统附带的使用说明并根据第3款和第6款使用此类系统。

2. Deployers shall assign human oversight to natural persons who have the necessary competence, training and authority, as well as the necessary support.

3. The obligations set out in paragraphs 1 and 2, are without prejudice to other deployer obligations under Union or national law and to the deployer's freedom to organise its own resources and activities for the purpose of implementing the human oversight measures indicated by the provider.

4. Without prejudice to paragraphs 1 and 2, to the extent the deployer exercises control over the input data, that deployer shall ensure that input data is relevant and sufficiently representative in view of the intended purpose of the high-risk AI system.

5. Deployers shall monitor the operation of the high-risk AI system on the basis of the instructions for use and, where relevant, inform providers in accordance with Article 72. Where deployers have reason to consider that the use of the high-risk AI system in accordance with the instructions may result in that AI system presenting a risk within the meaning of Article 79(1), they shall, without undue delay, inform the provider or distributor and the relevant market surveillance authority, and shall suspend the use of that system. Where deployers have identified a serious incident, they shall also immediately inform first the provider, and then the importer or distributor and the relevant market surveillance authorities of that incident. If the deployer is not able to reach the provider, Article 73 shall apply *mutatis mutandis*. This obligation shall not cover sensitive operational data of deployers of AI systems which are law enforcement authorities.

For deployers that are financial institutions subject to requirements regarding their internal governance, arrangements or processes under Union financial services law, the monitoring obligation set out in the first subparagraph shall be deemed to be fulfilled by complying with the rules on internal governance arrangements, processes and mechanisms pursuant to the relevant financial service law.

6. Deployers of high-risk AI systems shall keep the logs automatically generated by that high-risk AI system to the extent such logs are under their control, for a period appropriate to the intended purpose of the high-risk AI system, of at least six months, unless provided otherwise in applicable Union or national law, in particular in Union law on the protection of personal data.

Deployers that are financial institutions subject to requirements regarding their internal governance, arrangements or processes under Union financial services law shall maintain the logs as part of the documentation kept pursuant to the relevant Union financial service law.

7. Before putting into service or using a high-risk AI system at the workplace, deployers who are employers shall inform workers' representatives and the affected workers that they will be subject to the use of the high-risk AI system. This information shall be provided, where applicable, in accordance with the rules and procedures laid down in Union and national law and practice on information of workers and their representatives.

8. Deployers of high-risk AI systems that are public authorities, or Union institutions, bodies, offices or agencies shall comply with the registration obligations referred to in Article 49. When such deployers find that the high-risk AI system that they envisage using has not been registered in the EU database referred to in Article 71, they shall not use that system and shall inform the provider or the distributor.

9. Where applicable, deployers of high-risk AI systems shall use the information provided under Article 13 of this Regulation to comply with their obligation to carry out a data protection impact assessment under Article 35 of Regulation (EU) 2016/679 or Article 27 of Directive (EU) 2016/680.

10. Without prejudice to Directive (EU) 2016/680, in the framework of an investigation for the targeted search of a person suspected or convicted of having committed a criminal offence, the deployer of a high-risk AI system for post-remote biometric identification shall request an authorisation, *ex ante*, or without undue delay and no later than 48 hours, by a judicial authority or an administrative authority whose decision is binding and subject to judicial review, for the use of that system, except when it is used for the initial identification of a potential suspect based on objective and verifiable facts directly linked to the offence. Each use shall be limited to what is strictly necessary for the investigation of a specific criminal offence.

If the authorisation requested pursuant to the first subparagraph is rejected, the use of the post-remote biometric identification system linked to that requested authorisation shall be stopped with immediate effect and the personal data linked to the use of the high-risk AI system for which the authorisation was requested shall be deleted.

2. 部署者应将人类监督分配给具备必要能力、培训和权限以及必要支持的自然人。

3. 第1款和第2款规定的义务不影响部署者根据欧盟法或国家法承担的其他义务，也不影响部署者为实施提供者指明的人类监督措施而自主组织自身资源和活动的自由。

4. 在不影响第1款和第2款的情况下，部署者在控制输入数据的范围内，应确保输入数据对于高风险人工智能系统的预期目的是相关的且具有充分代表性。

5. 部署者应根据使用说明监测高风险人工智能系统的运行，并在相关情况下依照第72条告知提供者。如部署者有理由认为按照使用说明使用高风险人工智能系统可能导致该人工智能系统存在第79(1)条意义上的风险，应毫不迟延地告知提供者或分销商及相关市场监督机构，并应暂停使用该系统。如部署者已识别出严重事件，还应立即首先告知提供者，然后告知进口商或分销商及相关市场监督机构该事件。如部署者无法联系到提供者，第73条应比照适用。该义务不涵盖作为执法机构的部署者的人工智能系统敏感运行数据。

对于属于金融机构且受欧盟金融服务法下有关其内部治理、安排或流程的要求约束的部署者，遵守相关金融服务法关于内部治理安排、流程和机制的规定即视为已履行第一项子段规定的监测义务。

6. 高风险人工智能系统的部署者应在日志处于其控制范围内的限度内，保存该高风险人工智能系统自动生成的日志，保存期限应与该高风险人工智能系统的预期目的相适应，且至少为六个月，除非适用的欧盟法或国家法另有规定，特别是欧盟关于个人数据保护的法律。

属于金融机构且受欧盟金融服务法下有关其内部治理、安排或流程的要求约束的部署者，应依照相关欧盟金融服务法保存的文档的一部分保存日志。

7. 在工作场所投入使用或使用高风险人工智能系统之前，作为雇主的部署者应告知工人代表和受影响的工人，他们将受到该高风险人工智能系统使用的影响。在适用情况下，该信息应依照欧盟法和国家法及实践中关于向工人及其代表提供信息的规则和程序提供。

8. 作为公共机关或欧盟机构、机关、办事处或团体的高风险人工智能系统部署者，应遵守第49条所述的登记义务。当此类部署者发现其拟使用的高风险人工智能系统未在第71条所述的欧盟数据库中登记时，不得使用该系统，并应通知提供者或分销商。

9. 在适用情况下，高风险人工智能系统的部署者应使用本条例第13条提供的信息，以履行其根据条例(EU) 2016/679第35条或指令(EU) 2016/680第27条进行数据保护影响评估的义务。

10.在不影响Directive(EU) 2016/680的情况下，在对涉嫌或被判犯有刑事罪行的人进行定向搜查的调查框架内，用于事后远程生物特征识别的高风险人工智能系统的部署者，应就该系统的使用，事先或在不无故拖延且不迟于48小时内，请求司法当局或决定具有约束力且受司法审查的行政当局的授权，除非该系统用于基于与罪行直接相关的客观且可核实的事实对潜在嫌疑人进行初步识别。每次使用应限于对特定刑事罪行进行调查所严格必要的范围。

如依据第一项子段请求的授权被拒绝，与该请求授权相关的远程生物特征识别后系统的使用应立即停止，且与请求授权的高风险人工智能系统使用相关的个人数据应予删除。

In no case shall such high-risk AI system for post-remote biometric identification be used for law enforcement purposes in an untargeted way, without any link to a criminal offence, a criminal proceeding, a genuine and present or genuine and foreseeable threat of a criminal offence, or the search for a specific missing person. It shall be ensured that no decision that produces an adverse legal effect on a person may be taken by the law enforcement authorities based solely on the output of such post-remote biometric identification systems.

This paragraph is without prejudice to Article 9 of Regulation (EU) 2016/679 and Article 10 of Directive (EU) 2016/680 for the processing of biometric data.

Regardless of the purpose or deployer, each use of such high-risk AI systems shall be documented in the relevant police file and shall be made available to the relevant market surveillance authority and the national data protection authority upon request, excluding the disclosure of sensitive operational data related to law enforcement. This subparagraph shall be without prejudice to the powers conferred by Directive (EU) 2016/680 on supervisory authorities.

Deployers shall submit annual reports to the relevant market surveillance and national data protection authorities on their use of post-remote biometric identification systems, excluding the disclosure of sensitive operational data related to law enforcement. The reports may be aggregated to cover more than one deployment.

Member States may introduce, in accordance with Union law, more restrictive laws on the use of post-remote biometric identification systems.

11. Without prejudice to Article 50 of this Regulation, deployers of high-risk AI systems referred to in Annex III that make decisions or assist in making decisions related to natural persons shall inform the natural persons that they are subject to the use of the high-risk AI system. For high-risk AI systems used for law enforcement purposes Article 13 of Directive (EU) 2016/680 shall apply.

12. Deployers shall cooperate with the relevant competent authorities in any action those authorities take in relation to the high-risk AI system in order to implement this Regulation.

Article 27

Fundamental rights impact assessment for high-risk AI systems

1. Prior to deploying a high-risk AI system referred to in Article 6(2), with the exception of high-risk AI systems intended to be used in the area listed in point 2 of Annex III, deployers that are bodies governed by public law, or are private entities providing public services, and deployers of high-risk AI systems referred to in points 5 (b) and (c) of Annex III, shall perform an assessment of the impact on fundamental rights that the use of such system may produce. For that purpose, deployers shall perform an assessment consisting of:

(a) a description of the deployer's processes in which the high-risk AI system will be used in line with its intended purpose;

(b) a description of the period of time within which, and the frequency with which, each high-risk AI system is intended to be used;

(c) the categories of natural persons and groups likely to be affected by its use in the specific context;

(d) the specific risks of harm likely to have an impact on the categories of natural persons or groups of persons identified pursuant to point (c) of this paragraph, taking into account the information given by the provider pursuant to Article 13;

(e) a description of the implementation of human oversight measures, according to the instructions for use;

(f) the measures to be taken in the case of the materialisation of those risks, including the arrangements for internal governance and complaint mechanisms.

此类用于远程生物特征识别后置应用的高风险人工智能系统在任何情况下均不得以无针对性的方式用于执法目的，即与刑事犯罪、刑事诉讼程序、真实且当前存在或真实且可预见的刑事犯罪威胁，或搜寻特定失踪人员没有任何关联。应确保执法当局不得仅依据此类远程生物特征识别后置系统的输出结果，作出对个人产生不利法律效果的决定。

本款不影响条例(EU) 2016/679第9条和指令(EU) 2016/680第10条关于生物特征数据处理的规定。

无论目的或部署者为何，每次使用此类高风险人工智能系统均应在相关警务档案中记录，并应相关市场监督机构和国家数据保护机构的要求提供，但不包括披露与执法相关的敏感行动数据。本项子段不影响指令(EU) 2016/680赋予监督机构的权力。

部署者应就其对远程生物特征识别后系统的使用向相关市场监督和国家数据保护机构提交年度报告，但不包括披露与执法相关的敏感行动数据。报告可汇总涵盖多次部署。

成员国可依照欧盟法律，就远程生物特征识别后系统的使用制定更严格的限制性法律。

11. 在不影响本条例第50条的情况下，附件III所述作出或协助作出与自然人有关的决定的高风险人工智能系统的部署者，应告知自然人其受到该高风险人工智能系统使用的影响。对于用于执法目的的高风险人工智能系统，应适用指令(EU) 2016/680第13条。

12. 部署者应与相关主管机关合作，配合其就高风险人工智能系统为实施本条例而采取的任何行动。

第27条

高风险人工智能系统的基本权利影响评估

1. 在部署第6(2)条所述高风险人工智能系统之前，除拟用于附件三第2点所列领域的高风险人工智能系统外，属于公法管辖机构的部署者或提供公共服务的私营实体，以及附件三第5(b)点和(c)点所述高风险人工智能系统的部署者，应当对此类系统的使用可能产生的基本权利影响进行评估。为此，部署者应当进行包含以下内容的评估：

(a) 对部署者将依照预期目的使用高风险人工智能系统的流程的描述；

(b) 对每个高风险人工智能系统预期使用的期限和频率的描述；

(c) 在特定情境下可能受其使用影响的自然人和群体类别；

(d) 可能对本款(c)项所确定的自然人或群体类别产生影响的特定损害风险，同时考虑提供者根据第13条提供的信息；

(e) 根据使用说明，对人类监督措施实施情况的描述；

(f) 在这些风险成为现实时拟采取的措施，包括内部治理安排和投诉机制。

2. The obligation laid down in paragraph 1 applies to the first use of the high-risk AI system. The deployer may, in similar cases, rely on previously conducted fundamental rights impact assessments or existing impact assessments carried out by provider. If, during the use of the high-risk AI system, the deployer considers that any of the elements listed in paragraph 1 has changed or is no longer up to date, the deployer shall take the necessary steps to update the information.

3. Once the assessment referred to in paragraph 1 of this Article has been performed, the deployer shall notify the market surveillance authority of its results, submitting the filled-out template referred to in paragraph 5 of this Article as part of the notification. In the case referred to in Article 46(1), deployers may be exempt from that obligation to notify.

4. If any of the obligations laid down in this Article is already met through the data protection impact assessment conducted pursuant to Article 35 of Regulation (EU) 2016/679 or Article 27 of Directive (EU) 2016/680, the fundamental rights impact assessment referred to in paragraph 1 of this Article shall complement that data protection impact assessment.

5. The AI Office shall develop a template for a questionnaire, including through an automated tool, to facilitate deployers in complying with their obligations under this Article in a simplified manner.

SECTION 4

Notifying authorities and notified bodies

Article 28

Notifying authorities

1. Each Member State shall designate or establish at least one notifying authority responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring. Those procedures shall be developed in cooperation between the notifying authorities of all Member States.

2. Member States may decide that the assessment and monitoring referred to in paragraph 1 is to be carried out by a national accreditation body within the meaning of, and in accordance with, Regulation (EC) No 765/2008.

3. Notifying authorities shall be established, organised and operated in such a way that no conflict of interest arises with conformity assessment bodies, and that the objectivity and impartiality of their activities are safeguarded.

4. Notifying authorities shall be organised in such a way that decisions relating to the notification of conformity assessment bodies are taken by competent persons different from those who carried out the assessment of those bodies.

5. Notifying authorities shall offer or provide neither any activities that conformity assessment bodies perform, nor any consultancy services on a commercial or competitive basis.

6. Notifying authorities shall safeguard the confidentiality of the information that they obtain, in accordance with Article 78.

7. Notifying authorities shall have an adequate number of competent personnel at their disposal for the proper performance of their tasks. Competent personnel shall have the necessary expertise, where applicable, for their function, in fields such as information technologies, AI and law, including the supervision of fundamental rights.

Article 29

Application of a conformity assessment body for notification

1. Conformity assessment bodies shall submit an application for notification to the notifying authority of the Member State in which they are established.

2. 第1款规定的义务适用于高风险人工智能系统的首次使用。在类似情况下，部署者可依据先前进行的基本权利影响评估或提供者已进行的现有影响评估。如果在高风险人工智能系统使用期间，部署者认为第1款所列任何要素已发生变化或不再是最新的，部署者应采取必要步骤更新信息。

3. 一旦完成本条第1款所述的评估，部署者应将其结果通知市场监督机构，并作为通知的一部分提交本条第5款所述的已填写模板。在第46(1)条所述情况下，部署者可免于该通知义务。

4. 如果本条规定的任何义务已通过根据条例(EU) 2016/679第35条或指令(EU) 2016/680第27条进行的数据保护影响评估得到履行，则本条第1款所述的基本权利影响评估应补充该数据保护影响评估。

5. AI Office应制定问卷模板，包括通过自动化工具，以便利部署者以简化方式遵守本条规定的义务。

第4节

通知机构和公告机构

第28条

通知机构

1. 每个成员国应指定或设立至少一个公告机构，负责建立和执行为合格评定机构进行评估、指定和通知及其监督的必要程序。这些程序应由所有成员国的公告机构合作制定。

2. 成员国可决定第1款所述的评估和监督由符合条例(EC) No 765/2008含义并依照该条例的国家认可机构进行。

3. 公告机构的设立、组织和运作方式应确保不与合格评定机构产生利益冲突，并保障其活动的客观性和公正性。

4. 公告机构的组织方式应确保与合格评定机构通知有关的决定由与对这些机构进行评估的人员不同的人员作出。

5. 公告机构不得在商业或竞争基础上提供或从事合格评定机构所进行的任何活动，也不得提供或从事任何咨询服务。

6. 公告机构应依照第78条保障其获得信息的保密性。

7. 公告机构应拥有足够数量的合格人员以妥善履行其任务。合格人员在其职能方面应具备必要的专业知识，在适用情况下，包括信息技术、人工智能和法律等领域，包括对基本权利的监督。

第29条

公告机构符合性评估机构的申请

1. 合格评定机构应向其所设立成员国的公告机构主管部门提交通知申请。

2. The application for notification shall be accompanied by a description of the conformity assessment activities, the conformity assessment module or modules and the types of AI systems for which the conformity assessment body claims to be competent, as well as by an accreditation certificate, where one exists, issued by a national accreditation body attesting that the conformity assessment body fulfils the requirements laid down in Article 31.

Any valid document related to existing designations of the applicant notified body under any other Union harmonisation legislation shall be added.

3. Where the conformity assessment body concerned cannot provide an accreditation certificate, it shall provide the notifying authority with all the documentary evidence necessary for the verification, recognition and regular monitoring of its compliance with the requirements laid down in Article 31.

4. For notified bodies which are designated under any other Union harmonisation legislation, all documents and certificates linked to those designations may be used to support their designation procedure under this Regulation, as appropriate. The notified body shall update the documentation referred to in paragraphs 2 and 3 of this Article whenever relevant changes occur, in order to enable the authority responsible for notified bodies to monitor and verify continuous compliance with all the requirements laid down in Article 31.

Article 30

Notification procedure

1. Notifying authorities may notify only conformity assessment bodies which have satisfied the requirements laid down in Article 31.

2. Notifying authorities shall notify the Commission and the other Member States, using the electronic notification tool developed and managed by the Commission, of each conformity assessment body referred to in paragraph 1.

3. The notification referred to in paragraph 2 of this Article shall include full details of the conformity assessment activities, the conformity assessment module or modules, the types of AI systems concerned, and the relevant attestation of competence. Where a notification is not based on an accreditation certificate as referred to in Article 29(2), the notifying authority shall provide the Commission and the other Member States with documentary evidence which attests to the competence of the conformity assessment body and to the arrangements in place to ensure that that body will be monitored regularly and will continue to satisfy the requirements laid down in Article 31.

4. The conformity assessment body concerned may perform the activities of a notified body only where no objections are raised by the Commission or the other Member States within two weeks of a notification by a notifying authority where it includes an accreditation certificate referred to in Article 29(2), or within two months of a notification by the notifying authority where it includes documentary evidence referred to in Article 29(3).

5. Where objections are raised, the Commission shall, without delay, enter into consultations with the relevant Member States and the conformity assessment body. In view thereof, the Commission shall decide whether the authorisation is justified. The Commission shall address its decision to the Member State concerned and to the relevant conformity assessment body.

Article 31

Requirements relating to notified bodies

1. A notified body shall be established under the national law of a Member State and shall have legal personality.

2. Notified bodies shall satisfy the organisational, quality management, resources and process requirements that are necessary to fulfil their tasks, as well as suitable cybersecurity requirements.

3. The organisational structure, allocation of responsibilities, reporting lines and operation of notified bodies shall ensure confidence in their performance, and in the results of the conformity assessment activities that the notified bodies conduct.

2. 通知申请应附有合格评定活动、合格评定模块以及合格评定机构声称具备能力的AI系统类型的说明，以及由国家认可机构颁发的、证明该合格评定机构满足第31条所规定要求的认可证书(如存在)。

还应附上与申请人公告机构根据任何其他欧盟协调立法现有指定相关的任何有效文件。

3. 如果相关合格评定机构无法提供认可证书，则应向通知机关提供核实、认可和定期监督其符合第31条所规定要求所需的所有文件证据。

4. 对于根据任何其他欧盟协调立法被指定的公告机构，与这些指定相关的所有文件和证书可酌情用于支持其根据本条例的指定程序。公告机构应当在本条第2款和第3款所述文件发生相关变更时更新该文件，以使负责公告机构的当局能够监督和核查其持续符合第31条规定的所有要求。

第30条

通知程序

1. 通知机关只能通知满足第31条所规定要求的合格评定机构。

2. 通知机关应使用委员会开发并管理的电子通知工具，向委员会和其他成员国通知第1款所述的每个合格评定机构。

3. 本条第2款所述通知应当包括合格评定活动、合格评定模块、相关人工智能系统类型以及相关能力证明的完整细节。如果通知不是基于第29(2)条所述认可证书，则通知当局应当向委员会和其他成员国提供书面证据，证明合格评定机构的能力以及为确保该机构将受到定期监督并继续满足第31条规定的要求而作出的安排。

4. 相关合格评定机构只有在以下情况下才能履行公告机构的职责：通知机关的通知中包含第29(2)条所述的认可证书时，委员会或其他成员国在两周内未提出异议；或通知机关的通知中包含第29(3)条所述的文件证据时，委员会或其他成员国在两个月内未提出异议。

5. 如提出异议，委员会应立即与相关成员国和合格评定机构进行磋商。据此，委员会应决定授权是否合理。委员会应将其决定通知相关成员国和相关合格评定机构。

第31条

对公告机构的要求

1. 公告机构应依据成员国的国家法律设立，并应具有法律人格。

2. 公告机构应满足履行其任务所必需的组织、质量管理、资源和流程要求，以及适当的网络安全要求。

3. 公告机构的组织结构、职责分配、报告路线和运作应确保对其绩效以及公告机构所开展的合格评定活动结果的信任。

4. Notified bodies shall be independent of the provider of a high-risk AI system in relation to which they perform conformity assessment activities. Notified bodies shall also be independent of any other operator having an economic interest in high-risk AI systems assessed, as well as of any competitors of the provider. This shall not preclude the use of assessed high-risk AI systems that are necessary for the operations of the conformity assessment body, or the use of such high-risk AI systems for personal purposes.

5. Neither a conformity assessment body, its top-level management nor the personnel responsible for carrying out its conformity assessment tasks shall be directly involved in the design, development, marketing or use of high-risk AI systems, nor shall they represent the parties engaged in those activities. They shall not engage in any activity that might conflict with their independence of judgement or integrity in relation to conformity assessment activities for which they are notified. This shall, in particular, apply to consultancy services.

6. Notified bodies shall be organised and operated so as to safeguard the independence, objectivity and impartiality of their activities. Notified bodies shall document and implement a structure and procedures to safeguard impartiality and to promote and apply the principles of impartiality throughout their organisation, personnel and assessment activities.

7. Notified bodies shall have documented procedures in place ensuring that their personnel, committees, subsidiaries, subcontractors and any associated body or personnel of external bodies maintain, in accordance with Article 78, the confidentiality of the information which comes into their possession during the performance of conformity assessment activities, except when its disclosure is required by law. The staff of notified bodies shall be bound to observe professional secrecy with regard to all information obtained in carrying out their tasks under this Regulation, except in relation to the notifying authorities of the Member State in which their activities are carried out.

8. Notified bodies shall have procedures for the performance of activities which take due account of the size of a provider, the sector in which it operates, its structure, and the degree of complexity of the AI system concerned.

9. Notified bodies shall take out appropriate liability insurance for their conformity assessment activities, unless liability is assumed by the Member State in which they are established in accordance with national law or that Member State is itself directly responsible for the conformity assessment.

10. Notified bodies shall be capable of carrying out all their tasks under this Regulation with the highest degree of professional integrity and the requisite competence in the specific field, whether those tasks are carried out by notified bodies themselves or on their behalf and under their responsibility.

11. Notified bodies shall have sufficient internal competences to be able effectively to evaluate the tasks conducted by external parties on their behalf. The notified body shall have permanent availability of sufficient administrative, technical, legal and scientific personnel who possess experience and knowledge relating to the relevant types of AI systems, data and data computing, and relating to the requirements set out in Section 2.

12. Notified bodies shall participate in coordination activities as referred to in Article 38. They shall also take part directly, or be represented in, European standardisation organisations, or ensure that they are aware and up to date in respect of relevant standards.

Article 32

Presumption of conformity with requirements relating to notified bodies

Where a conformity assessment body demonstrates its conformity with the criteria laid down in the relevant harmonised standards or parts thereof, the references of which have been published in the *Official Journal of the European Union*, it shall be presumed to comply with the requirements set out in Article 31 in so far as the applicable harmonised standards cover those requirements.

4. 公告机构应当独立于其执行合格评定活动所涉高风险人工智能系统的提供者。公告机构还应当独立于对所评估的高风险人工智能系统具有经济利益的任何其他运营者，以及提供者的任何竞争者。这不应妨碍使用合格评定机构运营所必需的已评估高风险人工智能系统，或为此类高风险人工智能系统的个人目的使用。

5. 合格评定机构、其最高管理层以及负责执行合格评定任务的人员，均不得直接参与高风险人工智能系统的设计、开发、营销或使用，亦不得代表从事上述活动的相关方。他们不得从事任何可能与其所获公告的合格评定活动相关的判断独立性或诚信性相冲突的活动。此规定尤其适用于咨询服务。

6. 公告机构的组织和运作应保障其活动的独立性、客观性和公正性。公告机构应记录并实施结构和程序，以保障公正性，并在其整个组织、人员和评定活动中促进和适用公正性原则。

7. 公告机构应制定有文件记录的程序，确保其人员、委员会、子公司、分包商以及外部机构的任何关联机构或人员，依照第78条，对在履行合格评定活动期间所获取的信息予以保密，除非法律要求披露。公告机构的工作人员有义务对其在依据本条例执行任务过程中获得的所有信息遵守职业保密，但与其开展活动所在成员国的公告机构相关的情形除外。

8. 公告机构应具备执行活动的程序，适当考虑提供者的规模、其经营的行业、其结构以及相关AI系统的复杂程度。

9. 公告机构应为其合格评定活动购买适当的责任保险，除非根据国家法律由其设立所在的成员国承担赔偿责任，或该成员国本身直接负责合格评定。

10. 公告机构应能够以最高程度的职业诚信和特定领域所需的专业能力执行本 Regulation 下的所有任务，无论这些任务是由公告机构自身执行还是以其名义并在其责任下执行。

11. 公告机构应具有足够的内部能力，以有效评估外部方以其名义执行的任务。公告机构应永久拥有足够的行政、技术、法律和科学人员，这些人员具备与相关类型的AI系统、数据和数据计算以及第2节所规定要求相关的经验和知识。

12. 公告机构应参与第38条所述的协调活动。它们还应直接参加欧洲标准化组织或被代表参加，或确保其了解并掌握相关标准的最新情况。

第32条

与公告机构相关要求的符合性推定

当合格评定机构证明其符合相关协调标准或其部分条款(其引用已在欧盟官方公报上公布)中规定的标准时，应推定其符合第31条规定的要求，前提是适用的协调标准涵盖这些要求。

Article 33

Subsidiaries of notified bodies and subcontracting

1. Where a notified body subcontracts specific tasks connected with the conformity assessment or has recourse to a subsidiary, it shall ensure that the subcontractor or the subsidiary meets the requirements laid down in Article 31, and shall inform the notifying authority accordingly.

2. Notified bodies shall take full responsibility for the tasks performed by any subcontractors or subsidiaries.

3. Activities may be subcontracted or carried out by a subsidiary only with the agreement of the provider. Notified bodies shall make a list of their subsidiaries publicly available.

4. The relevant documents concerning the assessment of the qualifications of the subcontractor or the subsidiary and the work carried out by them under this Regulation shall be kept at the disposal of the notifying authority for a period of five years from the termination date of the subcontracting.

Article 34

Operational obligations of notified bodies

1. Notified bodies shall verify the conformity of high-risk AI systems in accordance with the conformity assessment procedures set out in Article 43.

2. Notified bodies shall avoid unnecessary burdens for providers when performing their activities, and take due account of the size of the provider, the sector in which it operates, its structure and the degree of complexity of the high-risk AI system concerned, in particular in view of minimising administrative burdens and compliance costs for micro- and small enterprises within the meaning of Recommendation 2003/361/EC. The notified body shall, nevertheless, respect the degree of rigour and the level of protection required for the compliance of the high-risk AI system with the requirements of this Regulation.

3. Notified bodies shall make available and submit upon request all relevant documentation, including the providers' documentation, to the notifying authority referred to in Article 28 to allow that authority to conduct its assessment, designation, notification and monitoring activities, and to facilitate the assessment outlined in this Section.

Article 35

Identification numbers and lists of notified bodies

1. The Commission shall assign a single identification number to each notified body, even where a body is notified under more than one Union act.

2. The Commission shall make publicly available the list of the bodies notified under this Regulation, including their identification numbers and the activities for which they have been notified. The Commission shall ensure that the list is kept up to date.

Article 36

Changes to notifications

1. The notifying authority shall notify the Commission and the other Member States of any relevant changes to the notification of a notified body via the electronic notification tool referred to in Article 30(2).

2. The procedures laid down in Articles 29 and 30 shall apply to extensions of the scope of the notification.

For changes to the notification other than extensions of its scope, the procedures laid down in paragraphs (3) to (9) shall apply.

第33条

公告机构的子公司与分包

1. 如果公告机构将与合格评定相关的特定任务分包或利用子公司，则应确保分包商或子公司满足第31条所规定的要求，并应相应通知通知机关。

2. 公告机构应对任何分包商或子公司执行的任务承担全部责任。

3. 只有在提供者同意的情况下，才能分包活动或由子公司执行。公告机构应公开其子公司清单。

4. 有关分包商或子公司资格评估以及其在本 Regulation 下所开展工作的相关文件，应自分包终止之日起五年内由通知机关保存备查。

第34条

公告机构的运营义务

1. 公告机构应按照第43条规定的合格评定程序验证高风险人工智能系统的符合性。

2. 公告机构在开展活动时应避免给提供者造成不必要的负担，并适当考虑提供者的规模、其经营所在行业、其组织结构以及相关高风险人工智能系统的复杂程度，尤其应着眼于最大限度减少2003/361/EC建议所指微型和小型企业的行政负担和合规成本。但公告机构仍应遵守高风险人工智能系统符合本条例要求所需的严格程度和保护水平。

3. 公告机构应提供并应要求向第28条所述的通知机关提交所有相关文件，包括提供者的文件，以便该机关开展其评估、指定、通知和监督活动，并促进本节所述评估。

第35条

公告机构的识别编号和清单

1. 委员会应为每个公告机构分配一个唯一识别号，即使该机构根据多个欧盟法案被通知。

2. 委员会应公开根据本 Regulation 被通知的机构清单，包括其识别号及其被通知的活动。委员会应确保该清单保持最新。

第36条

通知的变更

1. 通知机关应通过第30(2)条所述的电子通知工具，将公告机构通知的任何相关变更通知委员会和其他成员国。

2. 第29条和第30条规定的程序应适用于通知范围的扩展。

对于除范围扩展以外的通知变更，应适用第(3)至第(9)款规定的程序。

3. Where a notified body decides to cease its conformity assessment activities, it shall inform the notifying authority and the providers concerned as soon as possible and, in the case of a planned cessation, at least one year before ceasing its activities. The certificates of the notified body may remain valid for a period of nine months after cessation of the notified body's activities, on condition that another notified body has confirmed in writing that it will assume responsibilities for the high-risk AI systems covered by those certificates. The latter notified body shall complete a full assessment of the high-risk AI systems affected by the end of that nine-month-period before issuing new certificates for those systems. Where the notified body has ceased its activity, the notifying authority shall withdraw the designation.

4. Where a notifying authority has sufficient reason to consider that a notified body no longer meets the requirements laid down in Article 31, or that it is failing to fulfil its obligations, the notifying authority shall without delay investigate the matter with the utmost diligence. In that context, it shall inform the notified body concerned about the objections raised and give it the possibility to make its views known. If the notifying authority comes to the conclusion that the notified body no longer meets the requirements laid down in Article 31 or that it is failing to fulfil its obligations, it shall restrict, suspend or withdraw the designation as appropriate, depending on the seriousness of the failure to meet those requirements or fulfil those obligations. It shall immediately inform the Commission and the other Member States accordingly.

5. Where its designation has been suspended, restricted, or fully or partially withdrawn, the notified body shall inform the providers concerned within 10 days.

6. In the event of the restriction, suspension or withdrawal of a designation, the notifying authority shall take appropriate steps to ensure that the files of the notified body concerned are kept, and to make them available to notifying authorities in other Member States and to market surveillance authorities at their request.

7. In the event of the restriction, suspension or withdrawal of a designation, the notifying authority shall:

(a) assess the impact on the certificates issued by the notified body;

(b) submit a report on its findings to the Commission and the other Member States within three months of having notified the changes to the designation;

(c) require the notified body to suspend or withdraw, within a reasonable period of time determined by the authority, any certificates which were unduly issued, in order to ensure the continuing conformity of high-risk AI systems on the market;

(d) inform the Commission and the Member States about certificates the suspension or withdrawal of which it has required;

(e) provide the national competent authorities of the Member State in which the provider has its registered place of business with all relevant information about the certificates of which it has required the suspension or withdrawal; that authority shall take the appropriate measures, where necessary, to avoid a potential risk to health, safety or fundamental rights.

8. With the exception of certificates unduly issued, and where a designation has been suspended or restricted, the certificates shall remain valid in one of the following circumstances:

(a) the notifying authority has confirmed, within one month of the suspension or restriction, that there is no risk to health, safety or fundamental rights in relation to certificates affected by the suspension or restriction, and the notifying authority has outlined a timeline for actions to remedy the suspension or restriction; or

(b) the notifying authority has confirmed that no certificates relevant to the suspension will be issued, amended or re-issued during the course of the suspension or restriction, and states whether the notified body has the capability of continuing to monitor and remain responsible for existing certificates issued for the period of the suspension or restriction; in the event that the notifying authority determines that the notified body does not have the capability to support existing certificates issued, the provider of the system covered by the certificate shall confirm in writing to the national competent authorities of the Member State in which it has its registered place of business, within three months of the suspension or restriction, that another qualified notified body is temporarily assuming the functions of the notified body to monitor and remain responsible for the certificates during the period of suspension or restriction.

3. 公告机构决定停止其合格评定活动的，应尽快通知公告机构和相关提供者；如属计划停止，应至少在停止活动前一年通知。公告机构的证书可在该公告机构停止活动后九个月内继续有效，条件为另一公告机构已书面确认其将承担这些证书所涵盖的高风险人工智能系统的相关责任。后一公告机构应在该九个月期限结束前完成对受影响高风险人工智能系统的全面评估，之后方可为这些系统颁发新证书。公告机构已停止活动的，公告机构应撤销其指定。

4. 公告机构有充分理由认为某公告机构不再符合第31条规定的各项要求，或未能履行其义务的，公告机构应毫不迟延地以最大勤勉对该事项进行调查。在此过程中，其应将提出的异议告知相关公告机构，并给予其陈述意见的机会。公告机构如认定该公告机构不再符合第31条规定的各项要求或未能履行其义务，应根据不符合这些要求或未履行这些义务的严重程度，酌情限制、暂停或撤销其指定。其应立即相应通知委员会和其他成员国。

5. 如果公告机构的指定被暂停、限制或全部或部分撤销，该公告机构应在10天内通知相关提供者。

6. 在指定被限制、暂停或撤销的情况下，通知机关应采取适当措施确保相关公告机构的档案得到保存，并应其他成员国的通知机关和市场监督机构的请求向其提供。

7. 在指定被限制、暂停或撤销的情况下，通知机关应：

(a) 评估对公告机构签发的证书的影响；

(b) 在通知指定变更后三个月内向委员会和其他成员国提交关于其调查结果的报告；

(c) 要求公告机构在主管机关确定的合理期限内，暂停或撤销任何不当签发的证书，以确保市场上高风险人工智能系统的持续符合性；

(d) 将其已要求暂停或撤销的证书告知委员会和成员国；

(e) 向提供者注册营业地所在成员国的国家主管机关提供其已要求暂停或撤销的证书的所有相关信息；该主管机关应在必要时采取适当措施，以避免对健康、安全或基本权利造成潜在风险。

8. 除不当签发的证书外，在指定被暂停或限制的情况下，证书在下列情形之一中应继续有效：

(a) 通知机关已在暂停或限制后一个月内确认，与受暂停或限制影响的证书相关的健康、安全或基本权利不存在风险，且通知机关已概述了补救暂停或限制的行动时间表；或

(b) 公告机构已确认，在暂停或限制期间，不会签发、修订或重新签发与暂停相关的证书，并说明公告机构是否有能力在暂停或限制期间继续监督并对已签发的现有证书保持负责；如果公告机构认定公告机构不具备支持已签发现有证书的能力，证书所涵盖系统的提供者应在暂停或限制后三个月内，以书面形式向其注册营业地所在成员国的国家主管机关确认，另一家合格公告机构正在临时承担公告机构的职能，在暂停或限制期间监督并对证书保持负责。

9. With the exception of certificates unduly issued, and where a designation has been withdrawn, the certificates shall remain valid for a period of nine months under the following circumstances:

(a) the national competent authority of the Member State in which the provider of the high-risk AI system covered by the certificate has its registered place of business has confirmed that there is no risk to health, safety or fundamental rights associated with the high-risk AI systems concerned; and

(b) another notified body has confirmed in writing that it will assume immediate responsibility for those AI systems and completes its assessment within 12 months of the withdrawal of the designation.

In the circumstances referred to in the first subparagraph, the national competent authority of the Member State in which the provider of the system covered by the certificate has its place of business may extend the provisional validity of the certificates for additional periods of three months, which shall not exceed 12 months in total.

The national competent authority or the notified body assuming the functions of the notified body affected by the change of designation shall immediately inform the Commission, the other Member States and the other notified bodies thereof.

Article 37

Challenge to the competence of notified bodies

1. The Commission shall, where necessary, investigate all cases where there are reasons to doubt the competence of a notified body or the continued fulfilment by a notified body of the requirements laid down in Article 31 and of its applicable responsibilities.

2. The notifying authority shall provide the Commission, on request, with all relevant information relating to the notification or the maintenance of the competence of the notified body concerned.

3. The Commission shall ensure that all sensitive information obtained in the course of its investigations pursuant to this Article is treated confidentially in accordance with Article 78.

4. Where the Commission ascertains that a notified body does not meet or no longer meets the requirements for its notification, it shall inform the notifying Member State accordingly and request it to take the necessary corrective measures, including the suspension or withdrawal of the notification if necessary. Where the Member State fails to take the necessary corrective measures, the Commission may, by means of an implementing act, suspend, restrict or withdraw the designation. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 98(2).

Article 38

Coordination of notified bodies

1. The Commission shall ensure that, with regard to high-risk AI systems, appropriate coordination and cooperation between notified bodies active in the conformity assessment procedures pursuant to this Regulation are put in place and properly operated in the form of a sectoral group of notified bodies.

2. Each notifying authority shall ensure that the bodies notified by it participate in the work of a group referred to in paragraph 1, directly or through designated representatives.

3. The Commission shall provide for the exchange of knowledge and best practices between notifying authorities.

9. 除不当签发的证书外，在指定被撤销的情况下，证书在下列情形下应在九个月内继续有效：

(a) 证书所涵盖的高风险人工智能系统的提供者注册营业地所在成员国的国家主管机关已确认，相关高风险人工智能系统不存在与健康、安全或基本权利相关的风险；且

(b) 另一公告机构已书面确认，其将立即对上述人工智能系统承担责任，并在指定撤销后12个月内完成其评估。

在第一款所述情形下，证书所涵盖系统的提供者营业地所在成员国的国家主管机关可将证书的临时有效性延长额外三个月期限，总计不得超过12个月。

承担受指定变更影响的公告机构职能的国家主管机关或公告机构应立即通知委员会、其他成员国和其他公告机构。

第37条

对公告机构权限的质疑

1. 委员会应在必要时调查所有有理由怀疑公告机构的能力或公告机构持续满足Article 31规定的要求及其适用职责的情况。

2. 通知机关应根据请求向委员会提供与相关公告机构的通知或能力维持有关的所有相关信息。

3. 委员会应确保根据本条在调查过程中获得的所有敏感信息按照Article 78予以保密处理。

4. 如果委员会认定某公告机构不符合或不再符合其公告要求，应相应通知公告成员国，并请其采取必要的纠正措施，包括在必要时暂停或撤销公告。如果成员国未能采取必要的纠正措施，委员会可通过实施法案暂停、限制或撤销该指定。该实施法案应按照第98(2)条所述的审查程序通过。

第38条

公告机构的协调

1. 委员会应确保就高风险人工智能系统而言，以公告机构部门小组的形式，在依据本条例参与合格评定程序的公告机构之间建立适当的协调与合作，并使其正常运作。

2. 每个通知机关应确保其通知的机构直接或通过指定代表参与第1款所述小组的工作。

3. 委员会应规定通知机关之间的知识和最佳实践交流。

Article 39

Conformity assessment bodies of third countries

Conformity assessment bodies established under the law of a third country with which the Union has concluded an agreement may be authorised to carry out the activities of notified bodies under this Regulation, provided that they meet the requirements laid down in Article 31 or they ensure an equivalent level of compliance.

SECTION 5

Standards, conformity assessment, certificates, registration

Article 40

Harmonised standards and standardisation deliverables

1. High-risk AI systems or general-purpose AI models which are in conformity with harmonised standards or parts thereof the references of which have been published in the *Official Journal of the European Union* in accordance with Regulation (EU) No 1025/2012 shall be presumed to be in conformity with the requirements set out in Section 2 of this Chapter or, as applicable, with the obligations set out in of Chapter V, Sections 2 and 3, of this Regulation, to the extent that those standards cover those requirements or obligations.

2. In accordance with Article 10 of Regulation (EU) No 1025/2012, the Commission shall issue, without undue delay, standardisation requests covering all requirements set out in Section 2 of this Chapter and, as applicable, standardisation requests covering obligations set out in Chapter V, Sections 2 and 3, of this Regulation. The standardisation request shall also ask for deliverables on reporting and documentation processes to improve AI systems' resource performance, such as reducing the high-risk AI system's consumption of energy and of other resources during its lifecycle, and on the energy-efficient development of general-purpose AI models. When preparing a standardisation request, the Commission shall consult the Board and relevant stakeholders, including the advisory forum.

When issuing a standardisation request to European standardisation organisations, the Commission shall specify that standards have to be clear, consistent, including with the standards developed in the various sectors for products covered by the existing Union harmonisation legislation listed in Annex I, and aiming to ensure that high-risk AI systems or general-purpose AI models placed on the market or put into service in the Union meet the relevant requirements or obligations laid down in this Regulation.

The Commission shall request the European standardisation organisations to provide evidence of their best efforts to fulfil the objectives referred to in the first and the second subparagraph of this paragraph in accordance with Article 24 of Regulation (EU) No 1025/2012.

3. The participants in the standardisation process shall seek to promote investment and innovation in AI, including through increasing legal certainty, as well as the competitiveness and growth of the Union market, to contribute to strengthening global cooperation on standardisation and taking into account existing international standards in the field of AI that are consistent with Union values, fundamental rights and interests, and to enhance multi-stakeholder governance ensuring a balanced representation of interests and the effective participation of all relevant stakeholders in accordance with Articles 5, 6, and 7 of Regulation (EU) No 1025/2012.

Article 41

Common specifications

1. The Commission may adopt, implementing acts establishing common specifications for the requirements set out in Section 2 of this Chapter or, as applicable, for the obligations set out in Sections 2 and 3 of Chapter V where the following conditions have been fulfilled:

(a) the Commission has requested, pursuant to Article 10(1) of Regulation (EU) No 1025/2012, one or more European standardisation organisations to draft a harmonised standard for the requirements set out in Section 2 of this Chapter, or, as applicable, for the obligations set out in Sections 2 and 3 of Chapter V, and:

(i) the request has not been accepted by any of the European standardisation organisations; or

第39条

第三国合格评定机构

依据与欧盟缔结协定的第三国法律设立的合格评定机构，可被授权依据本条例开展公告机构的活动，前提是其符合第31条规定的要求或确保同等水平的合规性。

第5节

标准、合格评定、证书、注册

第40条

协调标准与标准化交付成果

1. 符合协调标准或其部分内容的高风险人工智能系统或通用人工智能模型，且这些标准的引用已根据(EU) No 1025/2012号条例在欧盟官方公报上公布，应被推定符合本章第2节规定的要求，或在适用情况下符合本条例第五章第2节和第3节规定的义务，前提是这些标准涵盖这些要求或义务。

2. 根据(EU) No 1025/2012号条例第10条，委员会应及时发布涵盖本章第2节规定的所有要求的标准化请求，并在适用情况下发布涵盖本条例第五章第2节和第3节规定义务的标准化请求。标准化请求还应要求提供关于报告和文档流程的可交付成果，以改善人工智能系统的资源性能，例如减少高风险人工智能系统在其生命周期内的能源和其他资源消耗，以及关于通用人工智能模型能效开发的成果。在准备标准化请求时，委员会应咨询委员会和包括咨询论坛在内的相关利益相关方。

在向欧洲标准化组织发布标准化请求时，委员会应明确标准必须清晰、一致，包括与附件一所列现有欧盟协调立法所涵盖产品在各行业制定的标准一致，并旨在确保在欧盟市场投放或投入服务的高风险人工智能系统或通用人工智能模型符合本条例规定的相关要求或义务。

委员会应要求欧洲标准化组织依照(EU) No 1025/2012号条例第24条提供证据，证明其已尽最大努力实现本款第一和第二项所述目标。

3. 标准化过程的参与者应寻求促进人工智能领域的投资和创新，包括通过提高法律确定性，以及联盟市场的竞争力和增长，为加强标准化领域的全球合作作出贡献，并考虑人工智能领域符合联盟价值观、基本权利和利益的现有国际标准，并加强多利益相关方治理，确保根据(EU) No 1025/2012号条例第5条、第6条和第7条实现利益的平衡代表和所有相关利益相关方的有效参与。

第41条

通用规范

1. 委员会可通过实施法案，为本章Section 2规定的要求，或在适用情况下为Chapter V的Sections 2和3规定的义务，制定共同规范，前提是已满足下列条件：

(a) 委员会已依据Regulation(EU) No 1025/2012的Article 10(1)请求一个或多个欧洲标准化组织为本章Section 2规定的要求，或在适用情况下为Chapter V的Sections 2和3规定的义务起草协调标准，且：

(i) 该请求未被任何欧洲标准化组织接受；或

(ii) the harmonised standards addressing that request are not delivered within the deadline set in accordance with Article 10(1) of Regulation (EU) No 1025/2012; or

(iii) the relevant harmonised standards insufficiently address fundamental rights concerns; or

(iv) the harmonised standards do not comply with the request; and

(b) no reference to harmonised standards covering the requirements referred to in Section 2 of this Chapter or, as applicable, the obligations referred to in Sections 2 and 3 of Chapter V has been published in the *Official Journal of the European Union* in accordance with Regulation (EU) No 1025/2012, and no such reference is expected to be published within a reasonable period.

When drafting the common specifications, the Commission shall consult the advisory forum referred to in Article 67.

The implementing acts referred to in the first subparagraph of this paragraph shall be adopted in accordance with the examination procedure referred to in Article 98(2).

2. Before preparing a draft implementing act, the Commission shall inform the committee referred to in Article 22 of Regulation (EU) No 1025/2012 that it considers the conditions laid down in paragraph 1 of this Article to be fulfilled.

3. High-risk AI systems or general-purpose AI models which are in conformity with the common specifications referred to in paragraph 1, or parts of those specifications, shall be presumed to be in conformity with the requirements set out in Section 2 of this Chapter or, as applicable, to comply with the obligations referred to in Sections 2 and 3 of Chapter V, to the extent those common specifications cover those requirements or those obligations.

4. Where a harmonised standard is adopted by a European standardisation organisation and proposed to the Commission for the publication of its reference in the *Official Journal of the European Union*, the Commission shall assess the harmonised standard in accordance with Regulation (EU) No 1025/2012. When reference to a harmonised standard is published in the *Official Journal of the European Union*, the Commission shall repeal the implementing acts referred to in paragraph 1, or parts thereof which cover the same requirements set out in Section 2 of this Chapter or, as applicable, the same obligations set out in Sections 2 and 3 of Chapter V.

5. Where providers of high-risk AI systems or general-purpose AI models do not comply with the common specifications referred to in paragraph 1, they shall duly justify that they have adopted technical solutions that meet the requirements referred to in Section 2 of this Chapter or, as applicable, comply with the obligations set out in Sections 2 and 3 of Chapter V to a level at least equivalent thereto.

6. Where a Member State considers that a common specification does not entirely meet the requirements set out in Section 2 or, as applicable, comply with obligations set out in Sections 2 and 3 of Chapter V, it shall inform the Commission thereof with a detailed explanation. The Commission shall assess that information and, if appropriate, amend the implementing act establishing the common specification concerned.

Article 42

Presumption of conformity with certain requirements

1. High-risk AI systems that have been trained and tested on data reflecting the specific geographical, behavioural, contextual or functional setting within which they are intended to be used shall be presumed to comply with the relevant requirements laid down in Article 10(4).

2. High-risk AI systems that have been certified or for which a statement of conformity has been issued under a cybersecurity scheme pursuant to Regulation (EU) 2019/881 and the references of which have been published in the *Official Journal of the European Union* shall be presumed to comply with the cybersecurity requirements set out in Article 15 of this Regulation in so far as the cybersecurity certificate or statement of conformity or parts thereof cover those requirements.

(ii) 应对该请求的协调标准未在依据Regulation(EU) No 1025/2012的Article 10(1)设定的截止日期内交付；或

(iii) 相关协调标准未充分处理基本权利关切；或

(iv) 该协调标准不符合请求；且

(b) 涵盖本Chapter Section 2所述要求或在适用情况下涵盖Chapter V的Sections 2和3所述义务的协调标准的引用，尚未依据Regulation(EU) No 1025/2012在*Official Journal of the European Union*上发布，且预计不会在合理期限内发布此类引用。

在起草共同规范时，委员会应咨询第67条提及的咨询论坛。

本款第一项所述的实施法案应按照第98条第2款所述的审查程序通过。

2. 在编制实施法案草案之前，委员会应通知Regulation(EU) No 1025/2012的Article 22所述委员会，其认为本条第1款规定的条件已满足。

3. 符合第1款所述共同规范或其中部分规范的高风险人工智能系统或通用人工智能模型，应被推定符合本Chapter Section 2规定的要求，或在适用情况下遵守Chapter V的Sections 2和3所述的义务，前提是上述共同规范涵盖上述要求或上述义务。

4.当欧洲标准化组织通过一项协调标准并提议委员会在*Official Journal of the European Union*上公布其引用时，委员会应依照Regulation(EU) No 1025/2012评估该协调标准。当协调标准的引用在*Official Journal of the European Union*上公布时，委员会应废止第1款所述实施法案中涵盖本章第2节所规定相同要求或(视情况)第五章第2节和第3节所规定相同义务的部分。

5. 高风险人工智能系统或通用人工智能模型的提供者不符合第1款所述共同规范时，应适当说明其已采用满足本Chapter Section 2所述要求的技术解决方案，或在适用情况下以至少同等水平遵守Chapter V的Sections 2和3规定的义务。

6. 成员国认为某项共同规范未完全满足Section 2规定的要求，或在适用情况下未完全遵守Chapter V的Sections 2和3规定的义务时，应附详细说明通知委员会。委员会应评估该信息，并酌情修订确立相关共同规范的实施法案。

第42条

符合某些要求的推定

1. 已使用反映其预期使用特定地理、行为、情境或功能环境的数据进行训练和测试的高风险人工智能系统，应被推定符合Article 10(4)规定的相关要求。

2. 已依据Regulation(EU) 2019/881在网络安全计划下获得认证或已获发符合性声明、且其引用已在*Official Journal of the European Union*上发布的高风险人工智能系统，应被推定符合本条例Article 15规定的网络安全要求，前提是网络安全证书或符合性声明或其部分涵盖上述要求。

Article 43

Conformity assessment

1. For high-risk AI systems listed in point 1 of Annex III, where, in demonstrating the compliance of a high-risk AI system with the requirements set out in Section 2, the provider has applied harmonised standards referred to in Article 40, or, where applicable, common specifications referred to in Article 41, the provider shall opt for one of the following conformity assessment procedures based on:

(a) the internal control referred to in Annex VI; or

(b) the assessment of the quality management system and the assessment of the technical documentation, with the involvement of a notified body, referred to in Annex VII.

In demonstrating the compliance of a high-risk AI system with the requirements set out in Section 2, the provider shall follow the conformity assessment procedure set out in Annex VII where:

(a) harmonised standards referred to in Article 40 do not exist, and common specifications referred to in Article 41 are not available;

(b) the provider has not applied, or has applied only part of, the harmonised standard;

(c) the common specifications referred to in point (a) exist, but the provider has not applied them;

(d) one or more of the harmonised standards referred to in point (a) has been published with a restriction, and only on the part of the standard that was restricted.

For the purposes of the conformity assessment procedure referred to in Annex VII, the provider may choose any of the notified bodies. However, where the high-risk AI system is intended to be put into service by law enforcement, immigration or asylum authorities or by Union institutions, bodies, offices or agencies, the market surveillance authority referred to in Article 74(8) or (9), as applicable, shall act as a notified body.

2. For high-risk AI systems referred to in points 2 to 8 of Annex III, providers shall follow the conformity assessment procedure based on internal control as referred to in Annex VI, which does not provide for the involvement of a notified body.

3. For high-risk AI systems covered by the Union harmonisation legislation listed in Section A of Annex I, the provider shall follow the relevant conformity assessment procedure as required under those legal acts. The requirements set out in Section 2 of this Chapter shall apply to those high-risk AI systems and shall be part of that assessment. Points 4.3., 4.4., 4.5. and the fifth paragraph of point 4.6 of Annex VII shall also apply.

For the purposes of that assessment, notified bodies which have been notified under those legal acts shall be entitled to control the conformity of the high-risk AI systems with the requirements set out in Section 2, provided that the compliance of those notified bodies with requirements laid down in Article 31(4), (5), (10) and (11) has been assessed in the context of the notification procedure under those legal acts.

Where a legal act listed in Section A of Annex I enables the product manufacturer to opt out from a third-party conformity assessment, provided that that manufacturer has applied all harmonised standards covering all the relevant requirements, that manufacturer may use that option only if it has also applied harmonised standards or, where applicable, common specifications referred to in Article 41, covering all requirements set out in Section 2 of this Chapter.

4. High-risk AI systems that have already been subject to a conformity assessment procedure shall undergo a new conformity assessment procedure in the event of a substantial modification, regardless of whether the modified system is intended to be further distributed or continues to be used by the current deployer.

For high-risk AI systems that continue to learn after being placed on the market or put into service, changes to the high-risk AI system and its performance that have been pre-determined by the provider at the moment of the initial conformity assessment and are part of the information contained in the technical documentation referred to in point 2(f) of Annex IV, shall not constitute a substantial modification.

5. The Commission is empowered to adopt delegated acts in accordance with Article 97 in order to amend Annexes VI and VII by updating them in light of technical progress.

第43条

合格评定

1. 对于附件三第1点所列的高风险人工智能系统，当提供者在证明高风险人工智能系统符合第2节规定的要求时，已适用第40条所述协调标准，或在适用情况下适用第41条所述通用规范，提供者应基于以下之一选择下列合格评定程序之一：

(a) 附件VI中提及的内部控制；或

(b) 质量管理体系的评估和技术文档的评估，并涉及公告机构，如附件七所述。

在证明高风险人工智能系统符合第2节规定的要求时，提供者应在以下情况下遵循附件七规定的合格评定程序：

(a) 第40条所述协调标准不存在，且第41条所述通用规范不可用；

(b) 提供者未适用或仅部分适用协调标准；

(c) 第(a)点所述通用规范存在，但提供者未适用；(d) 第(a)点所述一项或多项协调标准已发布但带有保留意见，且仅针对标准中被保留的部分。

就附件七所述的合格评定程序而言，提供者可选择任何公告机构。但是，如果高风险人工智能系统拟由执法、移民或庇护主管机关或由欧盟机构、机关、办事处或团体投入使用，则第74(8)条或第74(9)条(视适用情况)所述的市场监督机构应作为公告机构行事。

2. 对于附件三第2至8点所述高风险人工智能系统，提供者应遵循基于内部控制的合格评定程序，如附件六所述，该程序不涉及公告机构。

3. 对于附件一A节所列欧盟协调立法所涵盖的高风险人工智能系统，提供者应遵循这些法律法案所要求的相关合格评定程序。本章第2节规定的要求应适用于这些高风险人工智能系统，并应构成该评估的一部分。附件七第4.3、4.4、4.5点及第4.6点第五段也应适用。

为该评定的目的，已根据这些法律法案获得通知的公告机构应有权控制高风险人工智能系统对本第2节规定要求的符合性，前提是这些公告机构对第31(4)条、第31(5)条、第31(10)条和第31(11)条规定要求的遵守情况已在这些法律法案下的通知程序范围内得到评估。

如果附件一A节所列的某项法律法案使产品制造商能够选择不进行第三方合格评定，前提是该制造商已应用涵盖所有相关要求的全部协调标准，则该制造商只有在也已应用涵盖本章第2节规定的所有要求的协调标准或(在适用情况下)第41条所述的通用规范时，才可使用该选择权。

4. 已接受合格评定程序的高风险人工智能系统在发生实质性修改时，应接受新的合格评定程序，无论修改后的系统是否打算进一步分发或继续由当前部署者使用。

对于在投放市场或投入使用后继续学习的高风险人工智能系统，提供者在初始合格评定之时预先确定且属于附件四第2(f)点所述技术文档所含信息组成部分的对高风险人工智能系统及其性能的变更，不构成实质性修改。

5. 委员会有权根据第97条通过授权法案，以根据技术进步更新附件六和附件七的方式对其进行修订。

6. The Commission is empowered to adopt delegated acts in accordance with Article 97 in order to amend paragraphs 1 and 2 of this Article in order to subject high-risk AI systems referred to in points 2 to 8 of Annex III to the conformity assessment procedure referred to in Annex VII or parts thereof. The Commission shall adopt such delegated acts taking into account the effectiveness of the conformity assessment procedure based on internal control referred to in Annex VI in preventing or minimising the risks to health and safety and protection of fundamental rights posed by such systems, as well as the availability of adequate capacities and resources among notified bodies.

Article 44

Certificates

1. Certificates issued by notified bodies in accordance with Annex VII shall be drawn-up in a language which can be easily understood by the relevant authorities in the Member State in which the notified body is established.

2. Certificates shall be valid for the period they indicate, which shall not exceed five years for AI systems covered by Annex I, and four years for AI systems covered by Annex III. At the request of the provider, the validity of a certificate may be extended for further periods, each not exceeding five years for AI systems covered by Annex I, and four years for AI systems covered by Annex III, based on a re-assessment in accordance with the applicable conformity assessment procedures. Any supplement to a certificate shall remain valid, provided that the certificate which it supplements is valid.

3. Where a notified body finds that an AI system no longer meets the requirements set out in Section 2, it shall, taking account of the principle of proportionality, suspend or withdraw the certificate issued or impose restrictions on it, unless compliance with those requirements is ensured by appropriate corrective action taken by the provider of the system within an appropriate deadline set by the notified body. The notified body shall give reasons for its decision.

An appeal procedure against decisions of the notified bodies, including on conformity certificates issued, shall be available.

Article 45

Information obligations of notified bodies

1. Notified bodies shall inform the notifying authority of the following:

(a) any Union technical documentation assessment certificates, any supplements to those certificates, and any quality management system approvals issued in accordance with the requirements of Annex VII;

(b) any refusal, restriction, suspension or withdrawal of a Union technical documentation assessment certificate or a quality management system approval issued in accordance with the requirements of Annex VII;

(c) any circumstances affecting the scope of or conditions for notification;

(d) any request for information which they have received from market surveillance authorities regarding conformity assessment activities;

(e) on request, conformity assessment activities performed within the scope of their notification and any other activity performed, including cross-border activities and subcontracting.

2. Each notified body shall inform the other notified bodies of:

(a) quality management system approvals which it has refused, suspended or withdrawn, and, upon request, of quality system approvals which it has issued;

(b) Union technical documentation assessment certificates or any supplements thereto which it has refused, withdrawn, suspended or otherwise restricted, and, upon request, of the certificates and/or supplements thereto which it has issued.

6. 委员会有权根据第97条通过授权法案，以修订本条第1款和第2款，使附件三第2点至第8点所述高风险人工智能系统受附件七所述合格评定程序或其部分的约束。委员会在通过此类授权法案时，应考虑基于附件六所述内部控制的合格评定程序在预防或最大限度降低此类系统对健康和安全及基本权利保护所构成风险方面的有效性，以及公告机构是否具备充足的能力和资源。

第44条

证书

1. 公告机构根据附件七签发的证书应以公告机构所在成员国的相关主管当局易于理解的语言起草。

2. 证书在其所示期限内有效，对于附件一所涵盖的人工智能系统，该期限不得超过五年；对于附件三所涵盖的人工智能系统，该期限不得超过四年。应提供者请求，证书的有效期可基于依照适用合格评定程序进行的重新评估而进一步延长，每次延长期限对于附件一所涵盖的人工智能系统不得超过五年，对于附件三所涵盖的人工智能系统不得超过四年。证书的任何补充文件在其所补充的证书有效期间应保持有效。

3. 当公告机构发现人工智能系统不再符合第2节规定的要求时，应考虑到比例原则，暂停或撤销已签发的证书或对其施加限制，除非系统提供者在公告机构设定的适当期限内采取适当纠正措施确保符合这些要求。公告机构应说明其决定的理由。

应提供针对公告机构决定(包括关于已签发合格证书的决定)的申诉程序。

第45条

公告机构的信息义务

1. 公告机构应将以下事项告知公告主管机关：

(a) 根据附件七要求签发的任何欧盟技术文档评估证书、这些证书的任何补充文件，以及任何质量管理体系批准；

(b) 根据附件七要求签发的欧盟技术文档评估证书或质量管理体系批准的任何拒绝、限制、暂停或撤销；

(c) 任何影响通知范围或条件的情况；

(d) 其从市场监督机构收到的关于合格评定活动的任何信息请求；

(e) 应请求，在其通知范围内执行的合格评定活动以及执行的任何其他活动，包括跨境活动和分包。

2. 每个公告机构应告知其他公告机构：

(a) 其已拒绝、暂停或撤销的质量管理体系批准，以及应请求，其已签发的质量体系批准；

(b) 其已拒绝、撤销、暂停或以其他方式限制的欧盟技术文档评估证书或其任何补充文件，以及应请求，其已签发的证书和/或补充文件。

3. Each notified body shall provide the other notified bodies carrying out similar conformity assessment activities covering the same types of AI systems with relevant information on issues relating to negative and, on request, positive conformity assessment results.

4. Notified bodies shall safeguard the confidentiality of the information that they obtain, in accordance with Article 78.

Article 46

Derogation from conformity assessment procedure

1. By way of derogation from Article 43 and upon a duly justified request, any market surveillance authority may authorise the placing on the market or the putting into service of specific high-risk AI systems within the territory of the Member State concerned, for exceptional reasons of public security or the protection of life and health of persons, environmental protection or the protection of key industrial and infrastructural assets. That authorisation shall be for a limited period while the necessary conformity assessment procedures are being carried out, taking into account the exceptional reasons justifying the derogation. The completion of those procedures shall be undertaken without undue delay.

2. In a duly justified situation of urgency for exceptional reasons of public security or in the case of specific, substantial and imminent threat to the life or physical safety of natural persons, law-enforcement authorities or civil protection authorities may put a specific high-risk AI system into service without the authorisation referred to in paragraph 1, provided that such authorisation is requested during or after the use without undue delay. If the authorisation referred to in paragraph 1 is refused, the use of the high-risk AI system shall be stopped with immediate effect and all the results and outputs of such use shall be immediately discarded.

3. The authorisation referred to in paragraph 1 shall be issued only if the market surveillance authority concludes that the high-risk AI system complies with the requirements of Section 2. The market surveillance authority shall inform the Commission and the other Member States of any authorisation issued pursuant to paragraphs 1 and 2. This obligation shall not cover sensitive operational data in relation to the activities of law-enforcement authorities.

4. Where, within 15 calendar days of receipt of the information referred to in paragraph 3, no objection has been raised by either a Member State or the Commission in respect of an authorisation issued by a market surveillance authority of a Member State in accordance with paragraph 1, that authorisation shall be deemed justified.

5. Where, within 15 calendar days of receipt of the notification referred to in paragraph 3, objections are raised by a Member State against an authorisation issued by a market surveillance authority of another Member State, or where the Commission considers the authorisation to be contrary to Union law, or the conclusion of the Member States regarding the compliance of the system as referred to in paragraph 3 to be unfounded, the Commission shall, without delay, enter into consultations with the relevant Member State. The operators concerned shall be consulted and have the possibility to present their views. Having regard thereto, the Commission shall decide whether the authorisation is justified. The Commission shall address its decision to the Member State concerned and to the relevant operators.

6. Where the Commission considers the authorisation unjustified, it shall be withdrawn by the market surveillance authority of the Member State concerned.

7. For high-risk AI systems related to products covered by Union harmonisation legislation listed in Section A of Annex I, only the derogations from the conformity assessment established in that Union harmonisation legislation shall apply.

Article 47

EU declaration of conformity

1. The provider shall draw up a written machine readable, physical or electronically signed EU declaration of conformity for each high-risk AI system, and keep it at the disposal of the national competent authorities for 10 years after the high-risk AI system has been placed on the market or put into service. The EU declaration of conformity shall identify the high-risk AI system for which it has been drawn up. A copy of the EU declaration of conformity shall be submitted to the relevant national competent authorities upon request.

3. 每个公告机构应向开展涵盖相同类型人工智能系统的类似合格评定活动的其他公告机构提供有关否定性和应请求的肯定性合格评定结果问题的相关信息。

4. 公告机构应根据第78条保护其获得的信息的机密性。

第46条

对合格评定程序的克减

1. 作为对第43条的减损，经适当说明理由的请求，任何市场监督机构可出于公共安全或保护人的生命和健康、环境保护或保护关键工业和基础设施资产的例外原因，授权在有关成员国境内投放市场或投入使用特定高风险人工智能系统。该授权应在进行必要合格评定程序期间具有有限期限，同时考虑到证明减损正当的例外原因。上述程序应无不合理延迟地完成。

2. 在因公共安全例外原因而存在经适当说明理由的紧急情况，或存在对自然人的生命或人身安全的具体、重大和紧迫威胁的情况下，执法机构或民事保护机构可在未取得第1款所述授权的情况下投入使用特定高风险人工智能系统，但须在使用期间或使用后无不合理延迟地请求该授权。如第1款所述授权被拒绝，应立即停止使用该高风险人工智能系统，并立即丢弃此类使用的所有结果和输出。

3. 第1款所述授权仅应在市场监督机构认定高风险人工智能系统符合第2节要求时签发。市场监督机构应将根据第1款和第2款签发的任何授权通知委员会和其他成员国。该义务不涵盖与执法当局活动相关的敏感操作数据。

4. 如果在收到第3款所述信息后15个日历日内，成员国或委员会均未对成员国市场监督机构根据第1款签发的授权提出异议，则该授权应被视为合理。

5. 如在收到第3款所述通知后15个日历日内，一成员国对另一成员国市场监督机构签发的授权提出异议，或如委员会认为该授权违反欧盟法律，或认为成员国关于第3款所述系统合规性的结论缺乏依据，委员会应毫不延迟地与有关成员国进行磋商。应征求有关运营者的意见，并使其有机会陈述其观点。鉴于此，委员会应决定该授权是否正当。委员会应将其决定发送给有关成员国和有关运营者。

6. 如果委员会认为授权不合理，相关成员国的市场监督机构应予以撤销。

7. 对于与附件一A节所列欧盟协调立法所涵盖产品相关的高风险人工智能系统，仅适用该欧盟协调立法中确立的合格评定豁免。

第47条

欧盟符合性声明

1. 提供者应当为每一高风险人工智能系统起草一份书面、机器可读、经物理或电子签署的欧盟符合性声明，并在该高风险人工智能系统投放市场或投入使用后10年内，将其保存以供国家主管机关查阅。欧盟符合性声明应当标明其所针对的高风险人工智能系统。应相关国家主管机关的要求，应当提交欧盟符合性声明的副本。

2. The EU declaration of conformity shall state that the high-risk AI system concerned meets the requirements set out in Section 2. The EU declaration of conformity shall contain the information set out in Annex V, and shall be translated into a language that can be easily understood by the national competent authorities of the Member States in which the high-risk AI system is placed on the market or made available.

3. Where high-risk AI systems are subject to other Union harmonisation legislation which also requires an EU declaration of conformity, a single EU declaration of conformity shall be drawn up in respect of all Union law applicable to the high-risk AI system. The declaration shall contain all the information required to identify the Union harmonisation legislation to which the declaration relates.

4. By drawing up the EU declaration of conformity, the provider shall assume responsibility for compliance with the requirements set out in Section 2. The provider shall keep the EU declaration of conformity up-to-date as appropriate.

5. The Commission is empowered to adopt delegated acts in accordance with Article 97 in order to amend Annex V by updating the content of the EU declaration of conformity set out in that Annex, in order to introduce elements that become necessary in light of technical progress.

Article 48

CE marking

1. The CE marking shall be subject to the general principles set out in Article 30 of Regulation (EC) No 765/2008.

2. For high-risk AI systems provided digitally, a digital CE marking shall be used, only if it can easily be accessed via the interface from which that system is accessed or via an easily accessible machine-readable code or other electronic means.

3. The CE marking shall be affixed visibly, legibly and indelibly for high-risk AI systems. Where that is not possible or not warranted on account of the nature of the high-risk AI system, it shall be affixed to the packaging or to the accompanying documentation, as appropriate.

4. Where applicable, the CE marking shall be followed by the identification number of the notified body responsible for the conformity assessment procedures set out in Article 43. The identification number of the notified body shall be affixed by the body itself or, under its instructions, by the provider or by the provider's authorised representative. The identification number shall also be indicated in any promotional material which mentions that the high-risk AI system fulfils the requirements for CE marking.

5. Where high-risk AI systems are subject to other Union law which also provides for the affixing of the CE marking, the CE marking shall indicate that the high-risk AI system also fulfil the requirements of that other law.

Article 49

Registration

1. Before placing on the market or putting into service a high-risk AI system listed in Annex III, with the exception of high-risk AI systems referred to in point 2 of Annex III, the provider or, where applicable, the authorised representative shall register themselves and their system in the EU database referred to in Article 71.

2. Before placing on the market or putting into service an AI system for which the provider has concluded that it is not high-risk according to Article 6(3), that provider or, where applicable, the authorised representative shall register themselves and that system in the EU database referred to in Article 71.

3. Before putting into service or using a high-risk AI system listed in Annex III, with the exception of high-risk AI systems listed in point 2 of Annex III, deployers that are public authorities, Union institutions, bodies, offices or agencies or persons acting on their behalf shall register themselves, select the system and register its use in the EU database referred to in Article 71.

2. 欧盟符合性声明应声明相关高风险人工智能系统符合第2节规定的要求。欧盟符合性声明应包含附件V所列信息，并应翻译成高风险人工智能系统投放市场或提供所在成员国国家主管机关易于理解的语言。

3. 高风险人工智能系统受其他同样要求欧盟符合性声明的欧盟协调立法约束的，应就该高风险人工智能系统适用的所有欧盟法律拟定单一欧盟符合性声明。该声明应包含识别声明所涉欧盟协调立法所需的所有信息。

4. 提供者通过拟定欧盟符合性声明，应承担符合第2节规定要求的责任。提供者应酌情保持欧盟符合性声明的最新状态。

5. 委员会有权根据第97条通过授权法案，通过更新该附件所列欧盟符合性声明的内容来修订附件V，以引入因技术进步而变得必要的要素。

第48条

CE 标志

1. CE 标志应遵守(EC) No 765/2008号条例第30条规定的一般原则。

2. 对于以数字方式提供的高风险人工智能系统，应使用数字CE 标志，但仅限于可通过访问该系统的界面或通过易于访问的机器可读代码或其他电子方式轻松访问该标志的情况。

3. 高风险人工智能系统的CE 标志应清晰、易读且不可擦除地加贴。如因高风险人工智能系统的性质而无法或不宜加贴，则应酌情加贴于包装或随附文件上。

4. 在适用的情况下，CE 标志之后应附上负责 Article 43 规定的合格评定程序的公告机构的识别编号。公告机构的识别编号应由该机构自身或在其指示下由提供者或提供者的授权代表加贴。识别编号还应标注在提及该高风险人工智能系统符合 CE 标志要求的任何宣传材料中。

5. 高风险人工智能系统受其他同样规定加贴CE 标志的欧盟法律约束的，CE 标志应表明该高风险人工智能系统也符合该其他法律的要求。

第49条

登记

1. 在将附件III所列高风险人工智能系统(附件III第2点所述高风险人工智能系统除外)投放市场或投入使用之前，提供者或(如适用)授权代表应在第71条所述欧盟数据库中登记自身及其系统。

2. 在将提供者根据第6(3)条认定不属于高风险的人工智能系统投放市场或投入使用之前，该提供者或(如适用)授权代表应在第71条所述欧盟数据库中登记自身及该系统。

3. 在将附件III所列高风险人工智能系统(附件III第2点所列高风险人工智能系统除外)投入使用或使用之前，作为公共机构、欧盟机构、机关、办事处或团体或代表其行事的人员的部署者应在第71条所述欧盟数据库中登记自身、选择该系统并登记其使用情况。

4. For high-risk AI systems referred to in points 1, 6 and 7 of Annex III, in the areas of law enforcement, migration, asylum and border control management, the registration referred to in paragraphs 1, 2 and 3 of this Article shall be in a secure non-public section of the EU database referred to in Article 71 and shall include only the following information, as applicable, referred to in:

(a) Section A, points 1 to 10, of Annex VIII, with the exception of points 6, 8 and 9;

(b) Section B, points 1 to 5, and points 8 and 9 of Annex VIII;

(c) Section C, points 1 to 3, of Annex VIII;

(d) points 1, 2, 3 and 5, of Annex IX.

Only the Commission and national authorities referred to in Article 74(8) shall have access to the respective restricted sections of the EU database listed in the first subparagraph of this paragraph.

5. High-risk AI systems referred to in point 2 of Annex III shall be registered at national level.

CHAPTER IV

TRANSPARENCY OBLIGATIONS FOR PROVIDERS AND DEPLOYERS OF CERTAIN AI SYSTEMS

Article 50

Transparency obligations for providers and deployers of certain AI systems

1. Providers shall ensure that AI systems intended to interact directly with natural persons are designed and developed in such a way that the natural persons concerned are informed that they are interacting with an AI system, unless this is obvious from the point of view of a natural person who is reasonably well-informed, observant and circumspect, taking into account the circumstances and the context of use. This obligation shall not apply to AI systems authorised by law to detect, prevent, investigate or prosecute criminal offences, subject to appropriate safeguards for the rights and freedoms of third parties, unless those systems are available for the public to report a criminal offence.

2. Providers of AI systems, including general-purpose AI systems, generating synthetic audio, image, video or text content, shall ensure that the outputs of the AI system are marked in a machine-readable format and detectable as artificially generated or manipulated. Providers shall ensure their technical solutions are effective, interoperable, robust and reliable as far as this is technically feasible, taking into account the specificities and limitations of various types of content, the costs of implementation and the generally acknowledged state of the art, as may be reflected in relevant technical standards. This obligation shall not apply to the extent the AI systems perform an assistive function for standard editing or do not substantially alter the input data provided by the deployer or the semantics thereof, or where authorised by law to detect, prevent, investigate or prosecute criminal offences.

3. Deployers of an emotion recognition system or a biometric categorisation system shall inform the natural persons exposed thereto of the operation of the system, and shall process the personal data in accordance with Regulations (EU) 2016/679 and (EU) 2018/1725 and Directive (EU) 2016/680, as applicable. This obligation shall not apply to AI systems used for biometric categorisation and emotion recognition, which are permitted by law to detect, prevent or investigate criminal offences, subject to appropriate safeguards for the rights and freedoms of third parties, and in accordance with Union law.

4. Deployers of an AI system that generates or manipulates image, audio or video content constituting a deep fake, shall disclose that the content has been artificially generated or manipulated. This obligation shall not apply where the use is authorised by law to detect, prevent, investigate or prosecute criminal offence. Where the content forms part of an evidently artistic, creative, satirical, fictional or analogous work or programme, the transparency obligations set out in this paragraph are limited to disclosure of the existence of such generated or manipulated content in an appropriate manner that does not hamper the display or enjoyment of the work.

Deployers of an AI system that generates or manipulates text which is published with the purpose of informing the public on matters of public interest shall disclose that the text has been artificially generated or manipulated. This obligation shall not apply where the use is authorised by law to detect, prevent, investigate or prosecute criminal offences or where the AI-generated content has undergone a process of human review or editorial control and where a natural or legal person holds editorial responsibility for the publication of the content.

4. 对于附件III第1、6和7点所述高风险人工智能系统，在执法、移民、庇护和边境管制管理领域，本条第1、2和3款所述登记应在第71条所述欧盟数据库的安全非公开部分进行，并应仅包含以下信息(如适用):

(a) 附件VIII A节第1至10点，第6、8和9点除外；

(b) 附件VIII第B节第1至5点及第8点和第9点；

(c) 附件VIII第C节第1至3点；

(d) Annex IX第1、2、3和5点。

只有委员会和第74(8)条所指的国家主管机关才有权访问本款第一项所列欧盟数据库的相应受限部分。

5. 附件III第2点所述高风险人工智能系统应在国家层面注册。

第四章

特定人工智能系统的提供者和部署者的透明度义务

第50条

特定人工智能系统的提供者和部署者的透明度义务

1. 提供者应确保旨在与自然人直接交互的人工智能系统的设计和开发方式，使相关自然人被告知他们正在与人工智能系统交互，除非从一名合理知情、善于观察且审慎的自然人的角度来看，考虑到使用的情形和背景，这一点是显而易见的。本义务不适用于经法律授权用于侦查、预防、调查或起诉刑事犯罪的人工智能系统，但须为第三方的权利和自由提供适当保障，除非这些系统可供公众用于举报刑事犯罪。

2. 生成合成音频、图像、视频或文本内容的人工智能系统(包括通用人工智能系统)的提供者，应确保人工智能系统的输出以机器可读格式标记，并可被检测为人工生成或操纵。提供者应确保其技术解决方案在技术可行的范围内有效、可互操作、稳健且可靠，同时考虑到各类内容的特殊性和局限性、实施成本以及相关技术标准中可能反映的普遍公认的最新水平。本义务不适用于以下情形：人工智能系统对标准编辑执行辅助功能，或未实质性改变部署者提供的输入数据或其语义，或经法律授权用于侦查、预防、调查或起诉刑事犯罪。

3. 情绪识别系统或生物特征分类系统的部署者，应告知暴露于该系统操作的自然人，并应视情况依照 Regulation (EU) 2016/679 和 (EU) 2018/1725 以及 Directive (EU) 2016/680 处理个人数据。本义务不适用于经法律允许用于侦查、预防或调查刑事犯罪的生物特征分类和情绪识别的人工智能系统，但须为第三方的权利和自由提供适当保障，并符合欧盟法律。

4. 生成或操纵构成深度伪造的图像、音频或视频内容的人工智能系统的部署者，应披露该内容已被人工生成或操纵。本义务不适用于经法律授权用于侦查、预防、调查或起诉刑事犯罪的使用情形。若该内容构成明显具有艺术性、创造性、讽刺性、虚构性或类似性质的作品或节目的一部分，则本段规定的透明度义务仅限于以不妨碍该作品的展示或欣赏的适当方式披露此类生成或操纵内容的存在。

生成或操纵文本并以告知公众公共利益事项为目的发布该文本的人工智能系统的部署者，应披露该文本系人工生成或操纵。该义务不适用于经法律授权用于侦查、预防、调查或起诉刑事犯罪的使用情形，也不适用于AI生成内容已经过人工审查或编辑控制程序且自然人或法人对内容发布承担编辑责任的情形。

5. The information referred to in paragraphs 1 to 4 shall be provided to the natural persons concerned in a clear and distinguishable manner at the latest at the time of the first interaction or exposure. The information shall conform to the applicable accessibility requirements.

6. Paragraphs 1 to 4 shall not affect the requirements and obligations set out in Chapter III, and shall be without prejudice to other transparency obligations laid down in Union or national law for deployers of AI systems.

7. The AI Office shall encourage and facilitate the drawing up of codes of practice at Union level to facilitate the effective implementation of the obligations regarding the detection and labelling of artificially generated or manipulated content. The Commission may adopt implementing acts to approve those codes of practice in accordance with the procedure laid down in Article 56 (6). If it deems the code is not adequate, the Commission may adopt an implementing act specifying common rules for the implementation of those obligations in accordance with the examination procedure laid down in Article 98(2).

CHAPTER V

GENERAL-PURPOSE AI MODELS

SECTION 1

Classification rules

Article 51

Classification of general-purpose AI models as general-purpose AI models with systemic risk

1. A general-purpose AI model shall be classified as a general-purpose AI model with systemic risk if it meets any of the following conditions:

(a) it has high impact capabilities evaluated on the basis of appropriate technical tools and methodologies, including indicators and benchmarks;

(b) based on a decision of the Commission, *ex officio* or following a qualified alert from the scientific panel, it has capabilities or an impact equivalent to those set out in point (a) having regard to the criteria set out in Annex XIII.

2. A general-purpose AI model shall be presumed to have high impact capabilities pursuant to paragraph 1, point (a), when the cumulative amount of computation used for its training measured in floating point operations is greater than 10^{25}.

3. The Commission shall adopt delegated acts in accordance with Article 97 to amend the thresholds listed in paragraphs 1 and 2 of this Article, as well as to supplement benchmarks and indicators in light of evolving technological developments, such as algorithmic improvements or increased hardware efficiency, when necessary, for these thresholds to reflect the state of the art.

Article 52

Procedure

1. Where a general-purpose AI model meets the condition referred to in Article 51(1), point (a), the relevant provider shall notify the Commission without delay and in any event within two weeks after that requirement is met or it becomes known that it will be met. That notification shall include the information necessary to demonstrate that the relevant requirement has been met. If the Commission becomes aware of a general-purpose AI model presenting systemic risks of which it has not been notified, it may decide to designate it as a model with systemic risk.

2. The provider of a general-purpose AI model that meets the condition referred to in Article 51(1), point (a), may present, with its notification, sufficiently substantiated arguments to demonstrate that, exceptionally, although it meets that requirement, the general-purpose AI model does not present, due to its specific characteristics, systemic risks and therefore should not be classified as a general-purpose AI model with systemic risk.

5. 第1至4款所述信息应至迟在首次交互或接触时以清晰且可区分的方式向相关自然人提供。该信息应符合适用的无障碍要求。

6. 第1至第4款不影响第三章规定的要求和义务，且不影响欧盟法律或国家法律为人工智能系统部署者规定的其他透明度义务。

7. 人工智能办公室应鼓励和促进在联盟层面制定行为准则，以促进有效履行关于检测和标注人工生成或操纵内容的义务。委员会可通过实施法案，按照Article 56(6)规定的程序批准这些行为准则。如果委员会认为该准则不充分，可按照Article 98(2)规定的审查程序通过实施法案，规定履行这些义务的共同规则。

第五章

通用人工智能模型

第1节

分类规则

第51条

将通用人工智能模型归类为具有系统性风险的通用人工智能模型

1. 通用人工智能模型在符合下列任一条件时，应被归类为具有系统性风险的通用人工智能模型：

(a) 其具有基于适当技术工具和方法(包括指标和基准)评估的高影响力能力；

(b) 基于委员会的决定，依职权或根据科学小组的合格警示，其具有与(a)点所列相当的能力或影响，并考虑附件XIII所列标准。

2. 当通用人工智能模型训练所用的累计计算量以浮点运算衡量大于 10^{25}时，应依据第1款(a)项推定该模型具有高影响能力。

3. 委员会应依照 Article 97 通过授权法案，修订本条第 1 款和第 2 款所列的阈值，并根据不断发展的技术进展(如算法改进或硬件效率提升)补充基准和指标，在必要时使这些阈值反映最新技术水平。

第52条

程序

1. 当通用人工智能模型满足Article 51(1) point (a)所述条件时，相关提供者应立即通知委员会，且在任何情况下应在该要求得到满足或获悉其将得到满足后两周内通知。该通知应包括证明相关要求已得到满足所必需的信息。如果委员会获悉存在其未被通知的呈现系统性风险的通用人工智能模型，可决定将其指定为具有系统性风险的模型。

2. 符合 Article 51(1) point (a) 所述条件的通用人工智能模型提供者，可在其通知中提出充分有据的论据，以证明该通用人工智能模型虽然满足该要求，但因其特定特征而例外地不构成系统性风险，因此不应被归类为具有系统性风险的通用人工智能模型。

3. Where the Commission concludes that the arguments submitted pursuant to paragraph 2 are not sufficiently substantiated and the relevant provider was not able to demonstrate that the general-purpose AI model does not present, due to its specific characteristics, systemic risks, it shall reject those arguments, and the general-purpose AI model shall be considered to be a general-purpose AI model with systemic risk.

4. The Commission may designate a general-purpose AI model as presenting systemic risks, *ex officio* or following a qualified alert from the scientific panel pursuant to Article 90(1), point (a), on the basis of criteria set out in Annex XIII.

The Commission is empowered to adopt delegated acts in accordance with Article 97 in order to amend Annex XIII by specifying and updating the criteria set out in that Annex.

5. Upon a reasoned request of a provider whose model has been designated as a general-purpose AI model with systemic risk pursuant to paragraph 4, the Commission shall take the request into account and may decide to reassess whether the general-purpose AI model can still be considered to present systemic risks on the basis of the criteria set out in Annex XIII. Such a request shall contain objective, detailed and new reasons that have arisen since the designation decision. Providers may request reassessment at the earliest six months after the designation decision. Where the Commission, following its reassessment, decides to maintain the designation as a general-purpose AI model with systemic risk, providers may request reassessment at the earliest six months after that decision.

6. The Commission shall ensure that a list of general-purpose AI models with systemic risk is published and shall keep that list up to date, without prejudice to the need to observe and protect intellectual property rights and confidential business information or trade secrets in accordance with Union and national law.

SECTION 2

Obligations for providers of general-purpose AI models

Article 53

Obligations for providers of general-purpose AI models

1. Providers of general-purpose AI models shall:

(a) draw up and keep up-to-date the technical documentation of the model, including its training and testing process and the results of its evaluation, which shall contain, at a minimum, the information set out in Annex XI for the purpose of providing it, upon request, to the AI Office and the national competent authorities;

(b) draw up, keep up-to-date and make available information and documentation to providers of AI systems who intend to integrate the general-purpose AI model into their AI systems. Without prejudice to the need to observe and protect intellectual property rights and confidential business information or trade secrets in accordance with Union and national law, the information and documentation shall:

(i) enable providers of AI systems to have a good understanding of the capabilities and limitations of the general-purpose AI model and to comply with their obligations pursuant to this Regulation; and

(ii) contain, at a minimum, the elements set out in Annex XII;

(c) put in place a policy to comply with Union law on copyright and related rights, and in particular to identify and comply with, including through state-of-the-art technologies, a reservation of rights expressed pursuant to Article 4(3) of Directive (EU) 2019/790;

(d) draw up and make publicly available a sufficiently detailed summary about the content used for training of the general-purpose AI model, according to a template provided by the AI Office.

3. 如果委员会认定依据第 2 款提交的论据不够充分有据，且相关提供者未能证明该通用人工智能模型因其特定特征而不构成系统性风险，委员会应驳回这些论据，该通用人工智能模型应被视为具有系统性风险的通用人工智能模型。

4. 委员会可依职权或根据科学小组依第90(1)条(a)点发出的合格警报，基于附件XIII所列标准，认定某通用人工智能模型构成系统性风险。

根据第97条，委员会被授权通过授权法案，以通过明确和更新附件十三中规定的标准来修订该附件。

5. 应其模型已依据第4款被指定为具有系统性风险的通用人工智能模型的提供者的合理请求，委员会应考虑该请求，并可决定根据Annex XIII规定的标准重新评估该通用人工智能模型是否仍可被视为呈现系统性风险。该请求应包含自指定决定以来出现的客观、详细且新的理由。提供者可在指定决定后最早六个月请求重新评估。如果委员会在重新评估后决定维持其作为具有系统性风险的通用人工智能模型的指定，提供者可在该决定后最早六个月请求重新评估。

6. 委员会应确保公布具有系统性风险的通用人工智能模型清单，并应保持该清单的最新状态，但不影响根据欧盟法和国家法律遵守和保护知识产权、保密商业信息或商业秘密的需要。

第2节

通用人工智能模型提供者的义务

第53条

通用人工智能模型提供者的义务

1. 通用-purpose AI模型提供者应：

(a) 起草并保持模型技术文档的最新状态，包括其训练和测试过程及其评估结果，该文档至少应包含附件XI所规定的信息，以便应要求向AI Office和国家主管机关提供；

(b) 起草、保持最新状态并向打算将通用人工智能模型集成到其人工智能系统中的人工智能系统提供者提供信息和文档。在不影响根据欧盟和国家法律遵守和保护知识产权、保密商业信息或商业秘密的需要的情况下，该信息和文档应：

(i) 使人工智能系统提供者能够充分了解通用人工智能模型的能力和局限性，并遵守其根据本条例承担的义务；以及

(ii) 至少包含Annex XII所列要素；

(c) 制定遵守欧盟版权及相关权利法律的政策，特别是识别并遵守根据Directive (EU) 2019/790第4(3)条表达的权利保留，包括通过最先进技术；

(d) 根据AI Office提供的模板，起草并公开提供关于通用人工智能模型训练所用内容的足够详细的摘要。

2. The obligations set out in paragraph 1, points (a) and (b), shall not apply to providers of AI models that are released under a free and open-source licence that allows for the access, usage, modification, and distribution of the model, and whose parameters, including the weights, the information on the model architecture, and the information on model usage, are made publicly available. This exception shall not apply to general-purpose AI models with systemic risks.

3. Providers of general-purpose AI models shall cooperate as necessary with the Commission and the national competent authorities in the exercise of their competences and powers pursuant to this Regulation.

4. Providers of general-purpose AI models may rely on codes of practice within the meaning of Article 56 to demonstrate compliance with the obligations set out in paragraph 1 of this Article, until a harmonised standard is published. Compliance with European harmonised standards grants providers the presumption of conformity to the extent that those standards cover those obligations. Providers of general-purpose AI models who do not adhere to an approved code of practice or do not comply with a European harmonised standard shall demonstrate alternative adequate means of compliance for assessment by the Commission.

5. For the purpose of facilitating compliance with Annex XI, in particular points 2 (d) and (e) thereof, the Commission is empowered to adopt delegated acts in accordance with Article 97 to detail measurement and calculation methodologies with a view to allowing for comparable and verifiable documentation.

6. The Commission is empowered to adopt delegated acts in accordance with Article 97(2) to amend Annexes XI and XII in light of evolving technological developments.

7. Any information or documentation obtained pursuant to this Article, including trade secrets, shall be treated in accordance with the confidentiality obligations set out in Article 78.

Article 54

Authorised representatives of providers of general-purpose AI models

1. Prior to placing a general-purpose AI model on the Union market, providers established in third countries shall, by written mandate, appoint an authorised representative which is established in the Union.

2. The provider shall enable its authorised representative to perform the tasks specified in the mandate received from the provider.

3. The authorised representative shall perform the tasks specified in the mandate received from the provider. It shall provide a copy of the mandate to the AI Office upon request, in one of the official languages of the institutions of the Union. For the purposes of this Regulation, the mandate shall empower the authorised representative to carry out the following tasks:

(a) verify that the technical documentation specified in Annex XI has been drawn up and all obligations referred to in Article 53 and, where applicable, Article 55 have been fulfilled by the provider;

(b) keep a copy of the technical documentation specified in Annex XI at the disposal of the AI Office and national competent authorities, for a period of 10 years after the general-purpose AI model has been placed on the market, and the contact details of the provider that appointed the authorised representative;

(c) provide the AI Office, upon a reasoned request, with all the information and documentation, including that referred to in point (b), necessary to demonstrate compliance with the obligations in this Chapter;

(d) cooperate with the AI Office and competent authorities, upon a reasoned request, in any action they take in relation to the general-purpose AI model, including when the model is integrated into AI systems placed on the market or put into service in the Union.

4. The mandate shall empower the authorised representative to be addressed, in addition to or instead of the provider, by the AI Office or the competent authorities, on all issues related to ensuring compliance with this Regulation.

2.第1款(a)项和(b)项规定的义务不适用于以下人工智能模型提供者：该模型根据允许访问、使用、修改和分发模型的自由和开源许可证发布，且其参数(包括权重、模型架构信息和模型使用信息)已公开提供。该例外不适用于具有系统性风险的通用人工智能模型。

3.通用人工智能模型提供者应在必要时与委员会和国家主管机关合作，以行使其根据本条例的职权和权力。

4. 通用人工智能模型的提供者可依据Article 56含义内的行为准则证明其遵守了本条第1款规定的义务，直至协调标准发布为止。遵守欧洲协调标准使提供者在这些标准涵盖这些义务的范围内获得符合性推定。不遵守已批准行为准则或不符合欧洲协调标准的通用人工智能模型提供者应证明其他适当的合规方式，供委员会评估。

5.为便于遵守附件XI，特别是其第2(d)项和第2(e)项，委员会有权根据第97条通过授权法案，详细规定测量和计算方法，以便提供可比较和可验证的文档。

6.委员会有权根据第97(2)条通过授权法案，根据不断发展的技术发展修订附件XI和XII。

7.根据本条获得的任何信息或文档，包括商业秘密，应按照第78条规定的保密义务处理。

第54条

通用人工智能模型提供者的授权代表

1.在将通用人工智能模型投放欧盟市场之前，在第三国设立的提供者应通过书面授权指定一名在欧盟设立的授权代表。

2. 提供者应使其授权代表能够执行提供者所授予授权中规定的任务。

3.授权代表应执行从提供者处收到的授权中规定的任务。应要求，其应以欧盟机构官方语言之一向AI Office提供授权副本。为本条例的目的，授权应赋予授权代表执行以下任务的权力：

(a) 核实附件XI规定的技术文档已起草，且提供者已履行第53条以及(如适用)第55条提及的所有义务；

(b) 在通用人工智能模型投放市场后10年内，将附件XI规定的技术文档副本以及指定授权代表的提供者的联系方式供AI Office和国家主管机关使用；

(c) 应合理请求，向AI Office提供证明遵守本章义务所需的所有信息和文档，包括(b)项提及的信息和文档；

(d) 应合理请求，与AI Office和主管机关合作，参与其就通用人工智能模型采取的任何行动，包括当该模型被集成到在欧盟投放市场或投入使用的人工智能系统中时。

4.授权应赋予授权代表在确保遵守本条例相关的所有问题上，除提供者之外或代替提供者，接受AI Office或主管机关联系的权利。

5. The authorised representative shall terminate the mandate if it considers or has reason to consider the provider to be acting contrary to its obligations pursuant to this Regulation. In such a case, it shall also immediately inform the AI Office about the termination of the mandate and the reasons therefor.

6. The obligation set out in this Article shall not apply to providers of general-purpose AI models that are released under a free and open-source licence that allows for the access, usage, modification, and distribution of the model, and whose parameters, including the weights, the information on the model architecture, and the information on model usage, are made publicly available, unless the general-purpose AI models present systemic risks.

SECTION 3

Obligations of providers of general-purpose AI models with systemic risk

Article 55

Obligations of providers of general-purpose AI models with systemic risk

1. In addition to the obligations listed in Articles 53 and 54, providers of general-purpose AI models with systemic risk shall:

(a) perform model evaluation in accordance with standardised protocols and tools reflecting the state of the art, including conducting and documenting adversarial testing of the model with a view to identifying and mitigating systemic risks;

(b) assess and mitigate possible systemic risks at Union level, including their sources, that may stem from the development, the placing on the market, or the use of general-purpose AI models with systemic risk;

(c) keep track of, document, and report, without undue delay, to the AI Office and, as appropriate, to national competent authorities, relevant information about serious incidents and possible corrective measures to address them;

(d) ensure an adequate level of cybersecurity protection for the general-purpose AI model with systemic risk and the physical infrastructure of the model.

2. Providers of general-purpose AI models with systemic risk may rely on codes of practice within the meaning of Article 56 to demonstrate compliance with the obligations set out in paragraph 1 of this Article, until a harmonised standard is published. Compliance with European harmonised standards grants providers the presumption of conformity to the extent that those standards cover those obligations. Providers of general-purpose AI models with systemic risks who do not adhere to an approved code of practice or do not comply with a European harmonised standard shall demonstrate alternative adequate means of compliance for assessment by the Commission.

3. Any information or documentation obtained pursuant to this Article, including trade secrets, shall be treated in accordance with the confidentiality obligations set out in Article 78.

SECTION 4

Codes of practice

Article 56

Codes of practice

1. The AI Office shall encourage and facilitate the drawing up of codes of practice at Union level in order to contribute to the proper application of this Regulation, taking into account international approaches.

2. The AI Office and the Board shall aim to ensure that the codes of practice cover at least the obligations provided for in Articles 53 and 55, including the following issues:

5.如果授权代表认为或有理由认为提供者违反其根据本条例承担的义务，则应终止授权。在此情况下，其还应立即通知AI Office授权终止及终止原因。

6.本条规定的义务不适用于以下通用人工智能模型提供者：该模型根据允许访问、使用、修改和分发模型的自由和开源许可证发布，且其参数(包括权重、模型架构信息和模型使用信息)已公开提供，除非该通用人工智能模型具有系统性风险。

第3节

具有系统性风险的通用人工智能模型提供者的义务

第55条

具有系统性风险的通用人工智能模型提供者的义务

1.除第53条和第54条所列义务外，具有系统性风险的通用人工智能模型提供者还应：

(a) 按照反映最先进水平的标准化协议和工具进行模型评估，包括对模型进行对抗性测试并记录，以识别和缓解系统性风险；

(b) 评估和缓解欧盟层面可能因具有系统性风险的通用人工智能模型的开发、投放市场或使用而产生的可能的系统性风险，包括其来源；

(c) 跟踪、记录并及时向AI Office以及酌情向国家主管机关报告有关严重事件的相关信息和可能的纠正措施；

(d) 确保具有系统性风险的通用人工智能模型及模型物理基础设施具备适当水平的网络安全保护。

2. 具有系统性风险的通用人工智能模型的提供者可依据Article 56含义内的行为准则证明其遵守了本条第1款规定的义务，直至协调标准发布为止。遵守欧洲协调标准使提供者在这些标准涵盖这些义务的范围内获得符合性推定。不遵守已批准行为准则或不符合欧洲协调标准的具有系统性风险的通用人工智能模型提供者应证明其他适当的合规方式，供委员会评估。

3.根据本条获得的任何信息或文档，包括商业秘密，应按照第78条规定的保密义务处理。

第4节

行为准则

第56条

行为准则

1.AI Office应鼓励和促进在欧盟层面制定行为准则，以促进本条例的正确适用，同时考虑国际做法。

2.AI Office和委员会应致力于确保行为准则至少涵盖第53条和第55条规定的义务，包括以下问题：

(a) the means to ensure that the information referred to in Article 53(1), points (a) and (b), is kept up to date in light of market and technological developments;

(b) the adequate level of detail for the summary about the content used for training;

(c) the identification of the type and nature of the systemic risks at Union level, including their sources, where appropriate;

(d) the measures, procedures and modalities for the assessment and management of the systemic risks at Union level, including the documentation thereof, which shall be proportionate to the risks, take into consideration their severity and probability and take into account the specific challenges of tackling those risks in light of the possible ways in which such risks may emerge and materialise along the AI value chain.

3. The AI Office may invite all providers of general-purpose AI models, as well as relevant national competent authorities, to participate in the drawing-up of codes of practice. Civil society organisations, industry, academia and other relevant stakeholders, such as downstream providers and independent experts, may support the process.

4. The AI Office and the Board shall aim to ensure that the codes of practice clearly set out their specific objectives and contain commitments or measures, including key performance indicators as appropriate, to ensure the achievement of those objectives, and that they take due account of the needs and interests of all interested parties, including affected persons, at Union level.

5. The AI Office shall aim to ensure that participants to the codes of practice report regularly to the AI Office on the implementation of the commitments and the measures taken and their outcomes, including as measured against the key performance indicators as appropriate. Key performance indicators and reporting commitments shall reflect differences in size and capacity between various participants.

6. The AI Office and the Board shall regularly monitor and evaluate the achievement of the objectives of the codes of practice by the participants and their contribution to the proper application of this Regulation. The AI Office and the Board shall assess whether the codes of practice cover the obligations provided for in Articles 53 and 55, and shall regularly monitor and evaluate the achievement of their objectives. They shall publish their assessment of the adequacy of the codes of practice.

The Commission may, by way of an implementing act, approve a code of practice and give it a general validity within the Union. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 98(2).

7. The AI Office may invite all providers of general-purpose AI models to adhere to the codes of practice. For providers of general-purpose AI models not presenting systemic risks this adherence may be limited to the obligations provided for in Article 53, unless they declare explicitly their interest to join the full code.

8. The AI Office shall, as appropriate, also encourage and facilitate the review and adaptation of the codes of practice, in particular in light of emerging standards. The AI Office shall assist in the assessment of available standards.

9. Codes of practice shall be ready at the latest by 2 May 2025. The AI Office shall take the necessary steps, including inviting providers pursuant to paragraph 7.

If, by 2 August 2025, a code of practice cannot be finalised, or if the AI Office deems it is not adequate following its assessment under paragraph 6 of this Article, the Commission may provide, by means of implementing acts, common rules for the implementation of the obligations provided for in Articles 53 and 55, including the issues set out in paragraph 2 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 98(2).

(a) 确保第53(1)条(a)项和(b)项提及的信息根据市场和技术发展保持最新状态的手段；

(b) 关于训练所用内容的摘要的适当详细程度；

(c) 酌情识别欧盟层面系统性风险的类型和性质，包括其来源；

(d) 在欧盟层面评估和管理系统性风险的措施、程序和方式，包括相关文档记录，应与风险相称，考虑其严重性和可能性，并考虑到此类风险可能沿人工智能价值链出现和显现的方式所带来的应对这些风险的具体挑战。

3. 人工智能办公室可邀请所有通用人工智能模型提供者以及相关国家主管机关参与制定行为准则。民间社会组织、业界、学术界和其他相关利益相关方，如下游提供者和独立专家，可支持该过程。

4. 人工智能办公室和委员会应致力于确保行为准则明确规定其具体目标，并包含承诺或措施(酌情包括关键绩效指标)，以确保实现这些目标，并确保其在欧盟层面适当考虑所有利益相关方(包括受影响人员)的需求和利益。

5. 人工智能办公室应致力于确保行为准则的参与者定期向人工智能办公室报告承诺和所采取措施的实施情况及其成果，包括酌情根据关键绩效指标进行衡量。关键绩效指标和报告承诺应反映各参与者之间规模和能力的差异。

6. 人工智能办公室和委员会应定期监测和评估参与者对行为准则目标的实现情况及其对本条例适当适用的贡献。人工智能办公室和委员会应评估行为准则是否涵盖第53条和第55条规定的义务，并应定期监测和评估其目标的实现情况。它们应公布对行为准则充分性的评估。

委员会可通过实施法案批准行为准则，并赋予其在欧盟内的一般效力。该实施法案应根据第98条第(2)款所述的审查程序通过。

7. 人工智能办公室可邀请所有通用人工智能模型提供者遵守行为准则。对于不构成系统性风险的通用人工智能模型提供者，该遵守可限于Article 53规定的义务，除非其明确声明有意加入完整准则。

8. 人工智能办公室应酌情鼓励和促进行为准则的审查和调整，特别是考虑到新兴标准。人工智能办公室应协助评估现有标准。

9. 行为准则应最迟于2025年5月2日准备就绪。人工智能办公室应采取必要步骤，包括依据第7段邀请提供者。

如果到2 August 2025行为准则无法最终确定，或者如果人工智能办公室根据本条第6款进行评估后认为其不充分，委员会可通过实施法案提供实施Article 53和Article 55规定义务的共同规则，包括本条第2款所列问题。这些实施法案应根据Article 98(2)所述的审查程序通过。

CHAPTER VI

MEASURES IN SUPPORT OF INNOVATION

Article 57

AI regulatory sandboxes

1. Member States shall ensure that their competent authorities establish at least one AI regulatory sandbox at national level, which shall be operational by 2 August 2026. That sandbox may also be established jointly with the competent authorities of other Member States. The Commission may provide technical support, advice and tools for the establishment and operation of AI regulatory sandboxes.

The obligation under the first subparagraph may also be fulfilled by participating in an existing sandbox in so far as that participation provides an equivalent level of national coverage for the participating Member States.

2. Additional AI regulatory sandboxes at regional or local level, or established jointly with the competent authorities of other Member States may also be established.

3. The European Data Protection Supervisor may also establish an AI regulatory sandbox for Union institutions, bodies, offices and agencies, and may exercise the roles and the tasks of national competent authorities in accordance with this Chapter.

4. Member States shall ensure that the competent authorities referred to in paragraphs 1 and 2 allocate sufficient resources to comply with this Article effectively and in a timely manner. Where appropriate, national competent authorities shall cooperate with other relevant authorities, and may allow for the involvement of other actors within the AI ecosystem. This Article shall not affect other regulatory sandboxes established under Union or national law. Member States shall ensure an appropriate level of cooperation between the authorities supervising those other sandboxes and the national competent authorities.

5. AI regulatory sandboxes established under paragraph 1 shall provide for a controlled environment that fosters innovation and facilitates the development, training, testing and validation of innovative AI systems for a limited time before their being placed on the market or put into service pursuant to a specific sandbox plan agreed between the providers or prospective providers and the competent authority. Such sandboxes may include testing in real world conditions supervised therein.

6. Competent authorities shall provide, as appropriate, guidance, supervision and support within the AI regulatory sandbox with a view to identifying risks, in particular to fundamental rights, health and safety, testing, mitigation measures, and their effectiveness in relation to the obligations and requirements of this Regulation and, where relevant, other Union and national law supervised within the sandbox.

7. Competent authorities shall provide providers and prospective providers participating in the AI regulatory sandbox with guidance on regulatory expectations and how to fulfil the requirements and obligations set out in this Regulation.

Upon request of the provider or prospective provider of the AI system, the competent authority shall provide a written proof of the activities successfully carried out in the sandbox. The competent authority shall also provide an exit report detailing the activities carried out in the sandbox and the related results and learning outcomes. Providers may use such documentation to demonstrate their compliance with this Regulation through the conformity assessment process or relevant market surveillance activities. In this regard, the exit reports and the written proof provided by the national competent authority shall be taken positively into account by market surveillance authorities and notified bodies, with a view to accelerating conformity assessment procedures to a reasonable extent.

8. Subject to the confidentiality provisions in Article 78, and with the agreement of the provider or prospective provider, the Commission and the Board shall be authorised to access the exit reports and shall take them into account, as appropriate, when exercising their tasks under this Regulation. If both the provider or prospective provider and the national competent authority explicitly agree, the exit report may be made publicly available through the single information platform referred to in this Article.

9. The establishment of AI regulatory sandboxes shall aim to contribute to the following objectives:

(a) improving legal certainty to achieve regulatory compliance with this Regulation or, where relevant, other applicable Union and national law;

第六章

支持创新的措施

第57条

AI监管沙盒

1. 成员国应确保其主管机关在国家层面建立至少一个人工智能监管沙盒，该沙盒应于2 August 2026投入运行。该沙盒也可与其他成员国的主管机关联合建立。委员会可为人工智能监管沙盒的建立和运行提供技术支持、建议和工具。

第一项子款规定的义务也可通过参与现有沙盒来履行，只要该参与为参与成员国提供同等水平的国家覆盖。

2. 也可在区域或地方层面建立额外的人工智能监管沙盒，或与其他成员国的主管机关联合建立。

3. 欧洲数据保护监督员也可为欧盟机构、机关、办公室和机构建立人工智能监管沙盒，并可根据本章行使国家主管机关的职责和任务。

4. 成员国应确保第1款和第2款所指的主管机关分配充足资源，以有效、及时地遵守本条。在适当情况下，国家主管机关应与其他相关机关合作，并可允许人工智能生态系统内的其他行为者参与。本条不影响根据联盟法或国内法设立的其他监管沙盒。成员国应确保监督这些其他沙盒的机关与国家主管机关之间保持适当程度的合作。

5. 根据第1款建立的人工智能监管沙盒应提供受控环境，以促进创新，并便利创新人工智能系统在投放市场或投入使用前，根据提供者或潜在提供者与主管机关商定的具体沙盒计划，在有限时间内进行开发、训练、测试和验证。此类沙盒可包括在其中监督的真实世界条件下的测试。

6. 主管机关应酌情在人工智能监管沙盒内提供指导、监督和支持，以识别风险，特别是对基本权利、健康和安全的风险，测试缓解措施及其在沙盒内监督的本条例义务和要求以及相关其他欧盟和国家法律方面的有效性。

7. 主管机关应向参与人工智能监管沙盒的提供者和潜在提供者提供关于监管期望以及如何履行本条例规定的要求和义务的指导。

应人工智能系统提供者或潜在提供者的请求，主管机关应提供在沙盒中成功开展的活动的书面证明。主管机关还应提供一份退出报告，详细说明在沙盒中开展的活动及相关结果和学习成果。提供者可使用此类文件，通过合格评定程序或相关市场监督活动证明其对本条例的遵守情况。在这方面，市场监督机构和公告机构应积极考虑国家主管机关提供的退出报告和书面证明，以期在合理程度上加快合格评定程序。

8. 在不影响第78条保密规定的前提下，并经提供者或潜在提供者同意，委员会和委员会应被授权访问退出报告，并在适当情况下在行使本条例规定的任务时予以考虑。如果提供者或潜在提供者与国家主管机关均明确同意，退出报告可通过本条所指的单一信息平台公开提供。

9. 人工智能监管沙盒的建立应旨在促进以下目标：

(a) 提高法律确定性，以实现对本条例或相关其他适用欧盟和国家法律的监管合规；

(b) supporting the sharing of best practices through cooperation with the authorities involved in the AI regulatory sandbox;

(c) fostering innovation and competitiveness and facilitating the development of an AI ecosystem;

(d) contributing to evidence-based regulatory learning;

(e) facilitating and accelerating access to the Union market for AI systems, in particular when provided by SMEs, including start-ups.

10. National competent authorities shall ensure that, to the extent the innovative AI systems involve the processing of personal data or otherwise fall under the supervisory remit of other national authorities or competent authorities providing or supporting access to data, the national data protection authorities and those other national or competent authorities are associated with the operation of the AI regulatory sandbox and involved in the supervision of those aspects to the extent of their respective tasks and powers.

11. The AI regulatory sandboxes shall not affect the supervisory or corrective powers of the competent authorities supervising the sandboxes, including at regional or local level. Any significant risks to health and safety and fundamental rights identified during the development and testing of such AI systems shall result in an adequate mitigation. National competent authorities shall have the power to temporarily or permanently suspend the testing process, or the participation in the sandbox if no effective mitigation is possible, and shall inform the AI Office of such decision. National competent authorities shall exercise their supervisory powers within the limits of the relevant law, using their discretionary powers when implementing legal provisions in respect of a specific AI regulatory sandbox project, with the objective of supporting innovation in AI in the Union.

12. Providers and prospective providers participating in the AI regulatory sandbox shall remain liable under applicable Union and national liability law for any damage inflicted on third parties as a result of the experimentation taking place in the sandbox. However, provided that the prospective providers observe the specific plan and the terms and conditions for their participation and follow in good faith the guidance given by the national competent authority, no administrative fines shall be imposed by the authorities for infringements of this Regulation. Where other competent authorities responsible for other Union and national law were actively involved in the supervision of the AI system in the sandbox and provided guidance for compliance, no administrative fines shall be imposed regarding that law.

13. The AI regulatory sandboxes shall be designed and implemented in such a way that, where relevant, they facilitate cross-border cooperation between national competent authorities.

14. National competent authorities shall coordinate their activities and cooperate within the framework of the Board.

15. National competent authorities shall inform the AI Office and the Board of the establishment of a sandbox, and may ask them for support and guidance. The AI Office shall make publicly available a list of planned and existing sandboxes and keep it up to date in order to encourage more interaction in the AI regulatory sandboxes and cross-border cooperation.

16. National competent authorities shall submit annual reports to the AI Office and to the Board, from one year after the establishment of the AI regulatory sandbox and every year thereafter until its termination, and a final report. Those reports shall provide information on the progress and results of the implementation of those sandboxes, including best practices, incidents, lessons learnt and recommendations on their setup and, where relevant, on the application and possible revision of this Regulation, including its delegated and implementing acts, and on the application of other Union law supervised by the competent authorities within the sandbox. The national competent authorities shall make those annual reports or abstracts thereof available to the public, online. The Commission shall, where appropriate, take the annual reports into account when exercising its tasks under this Regulation.

17. The Commission shall develop a single and dedicated interface containing all relevant information related to AI regulatory sandboxes to allow stakeholders to interact with AI regulatory sandboxes and to raise enquiries with competent authorities, and to seek non-binding guidance on the conformity of innovative products, services, business models embedding AI technologies, in accordance with Article 62(1), point (c). The Commission shall proactively coordinate with national competent authorities, where relevant.

(b) 通过与参与人工智能监管沙盒的机关合作，支持最佳实践的分享；

(c) 促进创新和竞争力，并便利人工智能生态系统的发展；

(d) 有助于基于证据的监管学习；

(e) 便利和加速人工智能系统进入欧盟市场，特别是由SME(包括初创企业)提供的人工智能系统。

10. 国家主管机关应确保，在创新人工智能系统涉及个人数据处理或在其他方面属于提供或支持数据访问的其他国家当局或主管机关的监督职权范围时，国家数据保护当局及该等其他国家当局或主管机关应参与人工智能监管沙盒的运作，并在各自任务和权限范围内参与对这些方面的监督。

11. 人工智能监管沙盒不影响监督沙盒的主管机关(包括区域或地方层面)的监督或纠正权力。在此类人工智能系统的开发和测试过程中发现的任何对健康和安全以及基本权利的重大风险，应得到适当的缓解。国家主管机关有权暂时或永久中止测试过程，或在无法有效缓解的情况下中止参与沙盒，并应将此类决定通知人工智能办公室。国家主管机关应在相关法律范围内行使监督权力，在实施针对特定人工智能监管沙盒项目的法律规定时运用其自由裁量权，以支持联盟内的人工智能创新。

12. 参与人工智能监管沙盒的提供者和潜在提供者，仍应根据适用的欧盟和国家责任法，对因在沙盒中进行的实验而对第三方造成的任何损害承担责任。但是，只要潜在提供者遵守其参与的特定计划和条款与条件，并善意遵循国家主管机关给出的指导，主管机关不得因违反本条例而对其处以行政罚款。如果负责其他欧盟和国家法律的其他主管机关积极参与了对沙盒中人工智能系统的监督，并提供了合规指导，则不得就该法律处以行政罚款。

13. 人工智能监管沙盒的设计和实施应酌情促进国家主管机关之间的跨境合作。

14. 国家主管机关应在委员会框架内协调其活动并开展合作。

15. 国家主管机关应将沙盒的建立情况通知人工智能办公室和委员会，并可请求其支持和指导。人工智能办公室应公开提供计划中和现有沙盒的清单，并保持更新，以鼓励人工智能监管沙盒中更多的互动和跨境合作。

16. 国家主管机关应自人工智能监管沙盒设立一年后起，每年向人工智能办公室和委员会提交年度报告，直至其终止，并提交一份最终报告。这些报告应提供有关这些沙盒实施进展和结果的信息，包括最佳实践、事件、经验教训以及关于其设立的建议，并在相关情况下，就本条例的适用和可能的修订(包括其授权法案和实施法案)以及就主管机关在沙盒内监督的其他欧盟法律的适用提出建议。国家主管机关应在线向公众提供这些年度报告或其摘要。委员会在行使本条例规定的任务时，应酌情考虑这些年度报告。

17. 委员会应开发一个单一且专用的接口，其中包含与人工智能监管沙盒相关的所有相关信息，以便利益相关者与人工智能监管沙盒互动、向主管机关提出询问，并根据第62(1)条第(c)点就嵌入人工智能技术的创新产品、服务、商业模式的合规性寻求不具约束力的指导。委员会应在相关情况下主动与国家主管机关协调。

Article 58

Detailed arrangements for, and functioning of, AI regulatory sandboxes

1. In order to avoid fragmentation across the Union, the Commission shall adopt implementing acts specifying the detailed arrangements for the establishment, development, implementation, operation and supervision of the AI regulatory sandboxes. The implementing acts shall include common principles on the following issues:

(a) eligibility and selection criteria for participation in the AI regulatory sandbox;

(b) procedures for the application, participation, monitoring, exiting from and termination of the AI regulatory sandbox, including the sandbox plan and the exit report;

(c) the terms and conditions applicable to the participants.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 98(2).

2. The implementing acts referred to in paragraph 1 shall ensure:

(a) that AI regulatory sandboxes are open to any applying provider or prospective provider of an AI system who fulfils eligibility and selection criteria, which shall be transparent and fair, and that national competent authorities inform applicants of their decision within three months of the application;

(b) that AI regulatory sandboxes allow broad and equal access and keep up with demand for participation; providers and prospective providers may also submit applications in partnerships with deployers and other relevant third parties;

(c) that the detailed arrangements for, and conditions concerning AI regulatory sandboxes support, to the best extent possible, flexibility for national competent authorities to establish and operate their AI regulatory sandboxes;

(d) that access to the AI regulatory sandboxes is free of charge for SMEs, including start-ups, without prejudice to exceptional costs that national competent authorities may recover in a fair and proportionate manner;

(e) that they facilitate providers and prospective providers, by means of the learning outcomes of the AI regulatory sandboxes, in complying with conformity assessment obligations under this Regulation and the voluntary application of the codes of conduct referred to in Article 95;

(f) that AI regulatory sandboxes facilitate the involvement of other relevant actors within the AI ecosystem, such as notified bodies and standardisation organisations, SMEs, including start-ups, enterprises, innovators, testing and experimentation facilities, research and experimentation labs and European Digital Innovation Hubs, centres of excellence, individual researchers, in order to allow and facilitate cooperation with the public and private sectors;

(g) that procedures, processes and administrative requirements for application, selection, participation and exiting the AI regulatory sandbox are simple, easily intelligible, and clearly communicated in order to facilitate the participation of SMEs, including start-ups, with limited legal and administrative capacities and are streamlined across the Union, in order to avoid fragmentation and that participation in an AI regulatory sandbox established by a Member State, or by the European Data Protection Supervisor is mutually and uniformly recognised and carries the same legal effects across the Union;

(h) that participation in the AI regulatory sandbox is limited to a period that is appropriate to the complexity and scale of the project and that may be extended by the national competent authority;

(i) that AI regulatory sandboxes facilitate the development of tools and infrastructure for testing, benchmarking, assessing and explaining dimensions of AI systems relevant for regulatory learning, such as accuracy, robustness and cybersecurity, as well as measures to mitigate risks to fundamental rights and society at large.

3. Prospective providers in the AI regulatory sandboxes, in particular SMEs and start-ups, shall be directed, where relevant, to pre-deployment services such as guidance on the implementation of this Regulation, to other value-adding services such as help with standardisation documents and certification, testing and experimentation facilities, European Digital Innovation Hubs and centres of excellence.

第58条

人工智能监管沙盒的详细安排和运作

1. 为避免整个欧盟的碎片化，委员会应通过实施法案，规定人工智能监管沙盒的建立、开发、实施、运行和监督的详细安排。实施法案应包括关于以下问题的共同原则：

(a) 参与人工智能监管沙盒的资格和选择标准；

(b) 人工智能监管沙盒的申请、参与、监测、退出和终止程序，包括沙盒计划和退出报告；

(c) 适用于参与者的条款和条件。

这些实施法案应按照第98(2)条所指的审查程序通过。

2. 第1款所指的实施法案应确保：

(a) 人工智能监管沙盒向任何符合资格和选择标准的申请提供者或人工智能系统潜在提供者开放，这些标准应透明且公平，且国家主管机关应在申请后三个月内将决定告知申请人；

(b) 人工智能监管沙盒允许广泛和平等的准入，并跟上参与需求；提供者和潜在提供者也可与部署者和其他相关第三方合作提交申请；

(c) 人工智能监管沙盒的详细安排和条件尽可能支持国家主管机关建立和运行其人工智能监管沙盒的灵活性；

(d) SME(包括初创企业)免费进入人工智能监管沙盒，不影响国家主管机关可以公平和相称方式收回的例外费用；

(e) 通过人工智能监管沙盒的学习成果，便利提供者和潜在提供者遵守本条例下的合格评定义务以及自愿适用Article 95所述行为准则；

(f) 人工智能监管沙盒促进人工智能生态系统中其他相关主体的参与，例如公告机构和标准化组织、SME(包括初创企业)、企业、创新者、测试和实验设施、研究和实验实验室以及欧洲数字创新中心、卓越中心、个人研究人员，以便允许和促进与公共和私营部门的合作；

(g) 申请、选择、参与和退出人工智能监管沙盒的程序、流程和行政要求应简单、易于理解并明确传达，以便利法律和行政能力有限的SME(包括初创企业)参与，并在全欧盟范围内实现简化，以避免碎片化，并且参与由成员国或欧洲数据保护监督机构设立的人工智能监管沙盒应得到相互和统一的承认，并在全欧盟范围内具有相同的法律效力；

(h) 参与人工智能监管沙盒的期限限于与项目的复杂性和规模相适应的期间，并可由国家主管机关延长；

(i) 人工智能监管沙盒促进用于测试、基准测试、评估和解释与监管学习相关的人工智能系统维度(如准确性、稳健性和网络安全)的工具和基础设施的开发，以及减轻对基本权利和整个社会风险的措施。

3. 人工智能监管沙盒中的潜在提供者，特别是SME和初创企业，应在相关情况下被引导至部署前服务，例如关于本法规实施的指导，以及其他增值服务，例如标准化文件和认证方面的帮助、测试和实验设施、欧洲数字创新中心和卓越中心。

4. Where national competent authorities consider authorising testing in real world conditions supervised within the framework of an AI regulatory sandbox to be established under this Article, they shall specifically agree the terms and conditions of such testing and, in particular, the appropriate safeguards with the participants, with a view to protecting fundamental rights, health and safety. Where appropriate, they shall cooperate with other national competent authorities with a view to ensuring consistent practices across the Union.

Article 59

Further processing of personal data for developing certain AI systems in the public interest in the AI regulatory sandbox

1. In the AI regulatory sandbox, personal data lawfully collected for other purposes may be processed solely for the purpose of developing, training and testing certain AI systems in the sandbox when all of the following conditions are met:

(a) AI systems shall be developed for safeguarding substantial public interest by a public authority or another natural or legal person and in one or more of the following areas:

(i) public safety and public health, including disease detection, diagnosis prevention, control and treatment and improvement of health care systems;

(ii) a high level of protection and improvement of the quality of the environment, protection of biodiversity, protection against pollution, green transition measures, climate change mitigation and adaptation measures;

(iii) energy sustainability;

(iv) safety and resilience of transport systems and mobility, critical infrastructure and networks;

(v) efficiency and quality of public administration and public services;

(b) the data processed are necessary for complying with one or more of the requirements referred to in Chapter III, Section 2 where those requirements cannot effectively be fulfilled by processing anonymised, synthetic or other non-personal data;

(c) there are effective monitoring mechanisms to identify if any high risks to the rights and freedoms of the data subjects, as referred to in Article 35 of Regulation (EU) 2016/679 and in Article 39 of Regulation (EU) 2018/1725, may arise during the sandbox experimentation, as well as response mechanisms to promptly mitigate those risks and, where necessary, stop the processing;

(d) any personal data to be processed in the context of the sandbox are in a functionally separate, isolated and protected data processing environment under the control of the prospective provider and only authorised persons have access to those data;

(e) providers can further share the originally collected data only in accordance with Union data protection law; any personal data created in the sandbox cannot be shared outside the sandbox;

(f) any processing of personal data in the context of the sandbox neither leads to measures or decisions affecting the data subjects nor does it affect the application of their rights laid down in Union law on the protection of personal data;

(g) any personal data processed in the context of the sandbox are protected by means of appropriate technical and organisational measures and deleted once the participation in the sandbox has terminated or the personal data has reached the end of its retention period;

(h) the logs of the processing of personal data in the context of the sandbox are kept for the duration of the participation in the sandbox, unless provided otherwise by Union or national law;

(i) a complete and detailed description of the process and rationale behind the training, testing and validation of the AI system is kept together with the testing results as part of the technical documentation referred to in Annex IV;

4. 当国家主管机关考虑授权在本条设立的人工智能监管沙盒框架内监督的真实世界条件下进行测试时，它们应与参与者具体商定此类测试的条款和条件，特别是适当的保障措施，以保护基本权利、健康和安全。在适当情况下，它们应与其他国家主管机关合作，以确保全欧盟范围内做法一致。

第59条

为公共利益开发某些人工智能系统而在人工智能监管中对个人数据的进一步处理

沙盒

1. 在人工智能监管沙盒中，为其他目的合法收集的个人数据仅可为在沙盒中开发、训练和测试某些人工智能系统的目的进行处理，且须满足以下所有条件：

(a) 人工智能系统应由公共机构或另一自然人或法人开发，以保障重大公共利益，并涉及以下一个或多个领域：

(i) 公共安全和公共卫生，包括疾病检测、诊断、预防、控制和治疗以及卫生保健系统的改进；

(ii) 高水平的环境保护和环境质量改善、生物多样性保护、污染防治、绿色转型措施、气候变化减缓和适应措施；

(iii) 能源可持续性；

(iv) 交通系统和出行、关键基础设施和网络的安全性和韧性；

(v) 公共行政和公共服务的效率与质量；

(b) 所处理的个人数据对于遵守Chapter III, Section 2中提及的一项或多项要求是必要的，且这些要求无法通过处理匿名化、合成或其他非个人数据有效满足；

(c) 存在有效的监测机制，以识别在沙盒实验期间是否可能产生Regulation(EU) 2016/679第35条和Regulation(EU) 2018/1725第39条所述的对数据主体权利和自由的任何高风险，以及迅速减轻这些风险并在必要时停止处理的响应机制；

(d) 在沙盒背景下处理的任何个人数据均处于潜在提供者控制下的功能分离、隔离和受保护的数据处理环境中，且仅授权人员可访问这些数据；

(e) 提供者仅可依照欧盟数据保护法进一步共享最初收集的数据；在沙盒中创建的任何个人数据不得在沙盒外共享；

(f) 在沙盒背景下对个人数据的任何处理既不导致影响数据主体的措施或决定，也不影响欧盟个人数据保护法所规定的其权利的适用；

(g) 在沙盒背景下处理的任何个人数据均通过适当的技术和组织措施加以保护，并在参与沙盒终止或个人数据达到保留期限后删除；

(h) 在沙盒背景下个人数据处理日志在参与沙盒期间保存，除非欧盟或国家法律另有规定；

(i) 人工智能系统训练、测试和验证过程的完整详细描述及其理由与测试结果一起保存，作为Annex IV所述技术文档的一部分；

(j) a short summary of the AI project developed in the sandbox, its objectives and expected results is published on the website of the competent authorities; this obligation shall not cover sensitive operational data in relation to the activities of law enforcement, border control, immigration or asylum authorities.

2. For the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and preventing threats to public security, under the control and responsibility of law enforcement authorities, the processing of personal data in AI regulatory sandboxes shall be based on a specific Union or national law and subject to the same cumulative conditions as referred to in paragraph 1.

3. Paragraph 1 is without prejudice to Union or national law which excludes processing of personal data for other purposes than those explicitly mentioned in that law, as well as to Union or national law laying down the basis for the processing of personal data which is necessary for the purpose of developing, testing or training of innovative AI systems or any other legal basis, in compliance with Union law on the protection of personal data.

Article 60

Testing of high-risk AI systems in real world conditions outside AI regulatory sandboxes

1. Testing of high-risk AI systems in real world conditions outside AI regulatory sandboxes may be conducted by providers or prospective providers of high-risk AI systems listed in Annex III, in accordance with this Article and the real-world testing plan referred to in this Article, without prejudice to the prohibitions under Article 5.

The Commission shall, by means of implementing acts, specify the detailed elements of the real-world testing plan. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 98(2).

This paragraph shall be without prejudice to Union or national law on the testing in real world conditions of high-risk AI systems related to products covered by Union harmonisation legislation listed in Annex I.

2. Providers or prospective providers may conduct testing of high-risk AI systems referred to in Annex III in real world conditions at any time before the placing on the market or the putting into service of the AI system on their own or in partnership with one or more deployers or prospective deployers.

3. The testing of high-risk AI systems in real world conditions under this Article shall be without prejudice to any ethical review that is required by Union or national law.

4. Providers or prospective providers may conduct the testing in real world conditions only where all of the following conditions are met:

(a) the provider or prospective provider has drawn up a real-world testing plan and submitted it to the market surveillance authority in the Member State where the testing in real world conditions is to be conducted;

(b) the market surveillance authority in the Member State where the testing in real world conditions is to be conducted has approved the testing in real world conditions and the real-world testing plan; where the market surveillance authority has not provided an answer within 30 days, the testing in real world conditions and the real-world testing plan shall be understood to have been approved; where national law does not provide for a tacit approval, the testing in real world conditions shall remain subject to an authorisation;

(c) the provider or prospective provider, with the exception of providers or prospective providers of high-risk AI systems referred to in points 1, 6 and 7 of Annex III in the areas of law enforcement, migration, asylum and border control management, and high-risk AI systems referred to in point 2 of Annex III has registered the testing in real world conditions in accordance with Article 71(4) with a Union-wide unique single identification number and with the information specified in Annex IX; the provider or prospective provider of high-risk AI systems referred to in points 1, 6 and 7 of Annex III in the areas of law enforcement, migration, asylum and border control management, has registered the testing in real-world conditions in the secure non-public section of the EU database according to Article 49(4), point (d), with a Union-wide unique single identification number and with the information specified therein; the provider or prospective provider of high-risk AI systems referred to in point 2 of Annex III has registered the testing in real-world conditions in accordance with Article 49(5);

(j) 在沙盒中开发的人工智能项目的简要摘要、其目标和预期结果公布在主管机关的网站上；该义务不涵盖与执法、边境管制、移民或庇护机关活动相关的敏感业务数据。

2. 为预防、调查、侦查或起诉刑事犯罪或执行刑事处罚(包括防范和预防对公共安全的威胁)之目的，在执法机关控制和负责下，人工智能监管沙盒中对个人数据的处理应基于特定的欧盟或国家法律，并须满足与第1款所述相同的累积条件。

3. 第1款不影响排除为该法律中未明确提及的其他目的处理个人数据的欧盟或国家法律，也不影响规定为开发、测试或训练创新人工智能系统所必需的个人数据处理依据的欧盟或国家法律或任何其他法律依据，但须遵守欧盟个人数据保护法。

第60条

在人工智能监管沙盒之外的真实世界条件下测试高风险人工智能系统

1. Annex III所列高风险人工智能系统的提供者或潜在提供者可依照本条和本条所述真实世界测试计划，在人工智能监管沙盒之外的真实世界条件下测试高风险人工智能系统，但不影响Article 5下的禁止规定。

委员会应通过实施法案规定真实世界测试计划的详细要素。这些实施法案应依照第98条第2款所述审查程序通过。

本款不影响欧盟或国家法律关于与附件一所列欧盟协调立法所涵盖产品相关的高风险人工智能系统在真实世界条件下测试的规定。

2. 提供者或潜在提供者可在人工智能系统投放市场或投入使用之前的任何时间，自行或与一个或多个部署者或潜在部署者合作，在真实世界条件下测试Annex III所述的高风险人工智能系统。

3. 本条下在真实世界条件下测试高风险人工智能系统不影响欧盟或国家法律要求的任何伦理审查。

4. 提供者或潜在提供者仅在满足以下所有条件时方可在真实世界条件下进行测试：

(a) 提供者或潜在提供者已制定真实世界测试计划并提交至将进行真实世界条件下测试的成员国市场监督机构；

(b) 拟在真实世界条件下进行测试的成员国市场监督机构已批准该真实世界条件下的测试及真实世界测试计划；市场监督机构未在30天内作出答复的，应视为该真实世界条件下的测试及真实世界测试计划已获批准；国家法律未规定默示批准的，真实世界条件下的测试仍须获得授权；

(c) 提供者或潜在提供者已依照Article 71(4)以全联盟唯一单一识别编号并附附件九规定的信息，注册了真实世界条件下的测试，但执法、移民、庇护和边境管制管理领域附件三第1、6和7点所述高风险人工智能系统以及附件三第2点所述高风险人工智能系统的提供者或潜在提供者除外；执法、移民、庇护和边境管制管理领域附件三第1、6和7点所述高风险人工智能系统的提供者或潜在提供者，已依照Article 49(4) point (d)在EU数据库的安全非公开部分以全联盟唯一单一识别编号并附其中规定的信息，注册了真实世界条件下的测试；附件三第2点所述高风险人工智能系统的提供者或潜在提供者已依照Article 49(5)注册了真实世界条件下的测试；

(d) the provider or prospective provider conducting the testing in real world conditions is established in the Union or has appointed a legal representative who is established in the Union;

(e) data collected and processed for the purpose of the testing in real world conditions shall be transferred to third countries only provided that appropriate and applicable safeguards under Union law are implemented;

(f) the testing in real world conditions does not last longer than necessary to achieve its objectives and in any case not longer than six months, which may be extended for an additional period of six months, subject to prior notification by the provider or prospective provider to the market surveillance authority, accompanied by an explanation of the need for such an extension;

(g) the subjects of the testing in real world conditions who are persons belonging to vulnerable groups due to their age or disability, are appropriately protected;

(h) where a provider or prospective provider organises the testing in real world conditions in cooperation with one or more deployers or prospective deployers, the latter have been informed of all aspects of the testing that are relevant to their decision to participate, and given the relevant instructions for use of the AI system referred to in Article 13; the provider or prospective provider and the deployer or prospective deployer shall conclude an agreement specifying their roles and responsibilities with a view to ensuring compliance with the provisions for testing in real world conditions under this Regulation and under other applicable Union and national law;

(i) the subjects of the testing in real world conditions have given informed consent in accordance with Article 61, or in the case of law enforcement, where the seeking of informed consent would prevent the AI system from being tested, the testing itself and the outcome of the testing in the real world conditions shall not have any negative effect on the subjects, and their personal data shall be deleted after the test is performed;

(j) the testing in real world conditions is effectively overseen by the provider or prospective provider, as well as by deployers or prospective deployers through persons who are suitably qualified in the relevant field and have the necessary capacity, training and authority to perform their tasks;

(k) the predictions, recommendations or decisions of the AI system can be effectively reversed and disregarded.

5. Any subjects of the testing in real world conditions, or their legally designated representative, as appropriate, may, without any resulting detriment and without having to provide any justification, withdraw from the testing at any time by revoking their informed consent and may request the immediate and permanent deletion of their personal data. The withdrawal of the informed consent shall not affect the activities already carried out.

6. In accordance with Article 75, Member States shall confer on their market surveillance authorities the powers of requiring providers and prospective providers to provide information, of carrying out unannounced remote or on-site inspections, and of performing checks on the conduct of the testing in real world conditions and the related high-risk AI systems. Market surveillance authorities shall use those powers to ensure the safe development of testing in real world conditions.

7. Any serious incident identified in the course of the testing in real world conditions shall be reported to the national market surveillance authority in accordance with Article 73. The provider or prospective provider shall adopt immediate mitigation measures or, failing that, shall suspend the testing in real world conditions until such mitigation takes place, or otherwise terminate it. The provider or prospective provider shall establish a procedure for the prompt recall of the AI system upon such termination of the testing in real world conditions.

8. Providers or prospective providers shall notify the national market surveillance authority in the Member State where the testing in real world conditions is to be conducted of the suspension or termination of the testing in real world conditions and of the final outcomes.

9. The provider or prospective provider shall be liable under applicable Union and national liability law for any damage caused in the course of their testing in real world conditions.

(d) 进行真实世界条件下测试的提供者或潜在提供者在欧盟设立，或已任命一名在欧盟设立的法定代表人；

(e) 为真实世界条件下测试目的收集和处理的个人数据仅当实施欧盟法下适当且适用的保障措施时方可转移至第三国；

(f) 在真实世界条件下的测试持续时间不超过实现其目标所必需的时间，且在任何情况下不超过六个月，经提供者或潜在提供者事先通知市场监督机构并附上对此类延长期限必要性的说明，可再延长六个月；

(g) 因年龄或残疾而属于弱势群体的在真实世界条件下测试的受试者受到适当保护；

(h) 提供者或潜在提供者与一个或多个部署者或潜在部署者合作组织真实世界条件下的测试的，后者已被告知与其参与决定相关的测试的所有方面，并已获得Article 13所述人工智能系统的相关使用说明；提供者或潜在提供者与部署者或潜在部署者应订立协议，明确其角色和责任，以确保遵守本 Regulation 以及其他适用的 Union 和国家法律中关于真实世界条件下测试的规定；

(i) 在真实世界条件下测试的受试者已依照 Article 61 给予知情同意，或者在执法情况下，如果寻求知情同意将导致人工智能系统无法被测试，则测试本身及在真实世界条件下测试的结果不得对受试者产生任何负面影响，且其个人数据应在测试完成后删除；

(j) 在真实世界条件下的测试由提供者或潜在提供者以及部署者或潜在部署者通过具备相关领域适当资质并拥有履行其任务所需能力、培训和权限的人员进行有效监督；

(k) 人工智能系统的预测、建议或决定可以被有效撤销和忽略。

5. 在真实世界条件下测试的任何受试者，或经其合法指定的代表(视情况而定)，可随时通过撤回其知情同意退出测试，且不因此受到任何损害，也无需提供任何理由，并可要求立即永久删除其个人数据。撤回知情同意不影响已经开展的活动。

6. 根据第75条，成员国应授予其市场监督机构要求提供者和潜在提供者提供信息的权力、进行突击远程或现场检查的权力，以及对真实世界条件下测试的实施及相关高风险人工智能系统进行检查的权力。市场监督机构应利用这些权力确保真实世界条件下测试的安全开展。

7. 在真实世界条件下测试过程中发现的任何严重事件，应按照Article 73向国家市场监督机构报告。提供者或潜在提供者应立即采取缓解措施，若无法采取，则应暂停真实世界条件下的测试直至此类缓解措施到位，否则应终止测试。提供者或潜在提供者应建立程序，以便在真实世界条件下的测试终止时迅速召回该人工智能系统。

8. 提供者或潜在提供者应将真实世界条件下测试的中止或终止以及最终结果通知进行真实世界条件下测试的成员国的国家市场监督机构。

9. 提供者或潜在提供者应根据适用的欧盟和国家责任法，对在真实世界条件下测试过程中造成的任何损害承担责任。

Article 61

Informed consent to participate in testing in real world conditions outside AI regulatory sandboxes

1. For the purpose of testing in real world conditions under Article 60, freely-given informed consent shall be obtained from the subjects of testing prior to their participation in such testing and after their having been duly informed with concise, clear, relevant, and understandable information regarding:

(a) the nature and objectives of the testing in real world conditions and the possible inconvenience that may be linked to their participation;

(b) the conditions under which the testing in real world conditions is to be conducted, including the expected duration of the subject or subjects' participation;

(c) their rights, and the guarantees regarding their participation, in particular their right to refuse to participate in, and the right to withdraw from, testing in real world conditions at any time without any resulting detriment and without having to provide any justification;

(d) the arrangements for requesting the reversal or the disregarding of the predictions, recommendations or decisions of the AI system;

(e) the Union-wide unique single identification number of the testing in real world conditions in accordance with Article 60(4) point (c), and the contact details of the provider or its legal representative from whom further information can be obtained.

2. The informed consent shall be dated and documented and a copy shall be given to the subjects of testing or their legal representative.

Article 62

Measures for providers and deployers, in particular SMEs, including start-ups

1. Member States shall undertake the following actions:

(a) provide SMEs, including start-ups, having a registered office or a branch in the Union, with priority access to the AI regulatory sandboxes, to the extent that they fulfil the eligibility conditions and selection criteria; the priority access shall not preclude other SMEs, including start-ups, other than those referred to in this paragraph from access to the AI regulatory sandbox, provided that they also fulfil the eligibility conditions and selection criteria;

(b) organise specific awareness raising and training activities on the application of this Regulation tailored to the needs of SMEs including start-ups, deployers and, as appropriate, local public authorities;

(c) utilise existing dedicated channels and where appropriate, establish new ones for communication with SMEs including start-ups, deployers, other innovators and, as appropriate, local public authorities to provide advice and respond to queries about the implementation of this Regulation, including as regards participation in AI regulatory sandboxes;

(d) facilitate the participation of SMEs and other relevant stakeholders in the standardisation development process.

2. The specific interests and needs of the SME providers, including start-ups, shall be taken into account when setting the fees for conformity assessment under Article 43, reducing those fees proportionately to their size, market size and other relevant indicators.

3. The AI Office shall undertake the following actions:

(a) provide standardised templates for areas covered by this Regulation, as specified by the Board in its request;

(b) develop and maintain a single information platform providing easy to use information in relation to this Regulation for all operators across the Union;

第61条

在人工智能监管沙盒之外参与真实世界条件下测试的知情同意

1. 为第60条规定的真实世界条件下测试之目的，应在测试对象参与此类测试之前，并在其已就以下事项获得简明、清晰、相关且易于理解的信息之后，获得测试对象自由给出的知情同意：

(a) 真实世界条件下测试的性质和目标以及可能与其参与相关的可能不便；

(b) 在真实世界条件下进行测试的条件，包括受试者参与的预期持续时间；

(c) 其权利以及关于其参与的保障，特别是其拒绝参与的权利以及随时退出真实世界条件下测试的权利，且不因此受到任何损害，也无需提供任何理由；

(d) 请求推翻或忽略人工智能系统的预测、建议或决定的安排；

(e) 根据第60条第4款第(c)项的真实世界条件下测试的欧盟范围内唯一单一识别号，以及可从中获取进一步信息的提供者或其法律代表的联系方式。

2. 知情同意应注明日期并予以记录，副本应交给测试对象或其法律代表。

第62条

针对提供者和部署者，特别是中小企业(包括初创企业)的措施

1. 成员国应采取以下行动：

(a) 为在欧盟设有注册办事处或分支机构的中小企业(包括初创企业)提供优先进入人工智能监管沙盒的机会，前提是其满足资格条件和选择标准；优先进入不应妨碍本款所述以外的其他中小企业(包括初创企业)进入人工智能监管沙盒，前提是其也满足资格条件和选择标准；

(b) 针对中小企业(包括初创企业)、部署者以及酌情包括地方公共当局的需求，组织关于本条例适用的专项宣传和提高认识活动及培训活动；

(c) 利用现有的专用渠道，并在适当情况下建立新渠道，与中小企业(包括初创企业)、部署者、其他创新者以及酌情包括地方公共当局进行沟通，以提供建议并答复关于本条例实施的询问，包括关于参与人工智能监管沙盒的询问；

(d) 促进中小企业和其他相关利益相关者参与标准化制定过程。

2. 在设定第43条规定的合格评定费用时，应考虑中小企业提供者(包括初创企业)的具体利益和需求，按其规模、市场规模和其他相关指标相应减少费用。

3. AI Office 应采取以下行动：

(a) 为本条例所涵盖的领域提供标准化模板，具体由委员会在其请求中指定；

(b) 开发和维护一个单一信息平台，为全欧盟的所有运营者提供与本条例相关的易于使用的信息；

(c) organise appropriate communication campaigns to raise awareness about the obligations arising from this Regulation;

(d) evaluate and promote the convergence of best practices in public procurement procedures in relation to AI systems.

Article 63

Derogations for specific operators

1. Microenterprises within the meaning of Recommendation 2003/361/EC may comply with certain elements of the quality management system required by Article 17 of this Regulation in a simplified manner, provided that they do not have partner enterprises or linked enterprises within the meaning of that Recommendation. For that purpose, the Commission shall develop guidelines on the elements of the quality management system which may be complied with in a simplified manner considering the needs of microenterprises, without affecting the level of protection or the need for compliance with the requirements in respect of high-risk AI systems.

2. Paragraph 1 of this Article shall not be interpreted as exempting those operators from fulfilling any other requirements or obligations laid down in this Regulation, including those established in Articles 9, 10, 11, 12, 13, 14, 15, 72 and 73.

CHAPTER VII

GOVERNANCE

SECTION 1

Governance at Union level

Article 64

AI Office

1. The Commission shall develop Union expertise and capabilities in the field of AI through the AI Office.

2. Member States shall facilitate the tasks entrusted to the AI Office, as reflected in this Regulation.

Article 65

Establishment and structure of the European Artificial Intelligence Board

1. A European Artificial Intelligence Board (the 'Board') is hereby established.

2. The Board shall be composed of one representative per Member State. The European Data Protection Supervisor shall participate as observer. The AI Office shall also attend the Board's meetings, without taking part in the votes. Other national and Union authorities, bodies or experts may be invited to the meetings by the Board on a case by case basis, where the issues discussed are of relevance for them.

3. Each representative shall be designated by their Member State for a period of three years, renewable once.

4. Member States shall ensure that their representatives on the Board:

(a) have the relevant competences and powers in their Member State so as to contribute actively to the achievement of the Board's tasks referred to in Article 66;

(b) are designated as a single contact point vis-à-vis the Board and, where appropriate, taking into account Member States' needs, as a single contact point for stakeholders;

(c) 组织适当的沟通活动，以提高对本条例所产生义务的认识；

(d) 评估和促进与人工智能系统相关的公共采购程序中最佳实践的趋同。

第63条

特定运营商的例外规定

1. 2003/361/EC建议意义上的微型企业，只要其没有该建议意义上的合作企业或关联企业，可以简化方式遵守本 Regulation Article 17 所要求的质量管理体系的某些要素。为此，委员会应就质量管理体系中可简化遵守的要素制定指南，同时考虑微型企业的需求，且不影响保护水平或遵守高风险人工智能系统相关要求的需求。

2. 本条第一款不得被解释为免除这些运营者履行本条例规定的任何其他要求或义务，包括第9条、第10条、第11条、第12条、第13条、第14条、第15条、第72条和第73条所确立的要求或义务。

第七章

治理

第1节

联盟层面的治理

第64条

人工智能办公室

1. 委员会应通过人工智能办公室发展欧盟在人工智能领域的专业知识和能力。

2. 成员国应为本条例所反映的委托给人工智能办公室的任务提供便利。

第65条

欧洲人工智能委员会的设立和结构

1. 兹设立欧洲人工智能委员会(以下简称"委员会")。

2. 委员会应由每个成员国一名代表组成。欧洲数据保护监督员应以观察员身份参加。人工智能办公室也应出席委员会会议，但不参加表决。委员会可逐案邀请其他国家和欧盟当局、机构或专家参加会议，前提是所讨论的问题与其相关。

3. 每名代表应由其成员国指定，任期三年，可连任一次。

4. 成员国应确保其在委员会中的代表：

(a) 在其成员国拥有相关权限和权力，以便为第66条所述委员会任务的实现做出积极贡献；

(b) 被指定为与委员会对接的单一联络点，并在适当情况下，考虑到成员国的需求，被指定为利益相关者的单一联络点；

(c) are empowered to facilitate consistency and coordination between national competent authorities in their Member State as regards the implementation of this Regulation, including through the collection of relevant data and information for the purpose of fulfilling their tasks on the Board.

5. The designated representatives of the Member States shall adopt the Board's rules of procedure by a two-thirds majority. The rules of procedure shall, in particular, lay down procedures for the selection process, the duration of the mandate of, and specifications of the tasks of, the Chair, detailed arrangements for voting, and the organisation of the Board's activities and those of its sub-groups.

6. The Board shall establish two standing sub-groups to provide a platform for cooperation and exchange among market surveillance authorities and notifying authorities about issues related to market surveillance and notified bodies respectively.

The standing sub-group for market surveillance should act as the administrative cooperation group (ADCO) for this Regulation within the meaning of Article 30 of Regulation (EU) 2019/1020.

The Board may establish other standing or temporary sub-groups as appropriate for the purpose of examining specific issues. Where appropriate, representatives of the advisory forum referred to in Article 67 may be invited to such sub-groups or to specific meetings of those subgroups as observers.

7. The Board shall be organised and operated so as to safeguard the objectivity and impartiality of its activities.

8. The Board shall be chaired by one of the representatives of the Member States. The AI Office shall provide the secretariat for the Board, convene the meetings upon request of the Chair, and prepare the agenda in accordance with the tasks of the Board pursuant to this Regulation and its rules of procedure.

Article 66

Tasks of the Board

The Board shall advise and assist the Commission and the Member States in order to facilitate the consistent and effective application of this Regulation. To that end, the Board may in particular:

(a) contribute to the coordination among national competent authorities responsible for the application of this Regulation and, in cooperation with and subject to the agreement of the market surveillance authorities concerned, support joint activities of market surveillance authorities referred to in Article 74(11);

(b) collect and share technical and regulatory expertise and best practices among Member States;

(c) provide advice on the implementation of this Regulation, in particular as regards the enforcement of rules on general-purpose AI models;

(d) contribute to the harmonisation of administrative practices in the Member States, including in relation to the derogation from the conformity assessment procedures referred to in Article 46, the functioning of AI regulatory sandboxes, and testing in real world conditions referred to in Articles 57, 59 and 60;

(e) at the request of the Commission or on its own initiative, issue recommendations and written opinions on any relevant matters related to the implementation of this Regulation and to its consistent and effective application, including:

(i) on the development and application of codes of conduct and codes of practice pursuant to this Regulation, as well as of the Commission's guidelines;

(ii) the evaluation and review of this Regulation pursuant to Article 112, including as regards the serious incident reports referred to in Article 73, and the functioning of the EU database referred to in Article 71, the preparation of the delegated or implementing acts, and as regards possible alignments of this Regulation with the Union harmonisation legislation listed in Annex I;

(iii) on technical specifications or existing standards regarding the requirements set out in Chapter III, Section 2;

(c) 被授权促进其成员国内国家主管机关之间在本条例实施方面的一致性和协调，包括为此收集相关数据和信息以履行其在委员会中的任务。

5. 成员国指定的代表应以三分之二多数通过董事会的议事规则。议事规则应特别规定遴选程序、主席任期和任务规格、投票的详细安排以及董事会及其下属小组活动的组织。

6. 委员会应设立两个常设小组，分别为市场监督机构和公告机构就与市场监督和公告机构相关的问题提供合作与交流的平台。

市场监督常设小组应作为本条例在2019/1020号条例(EU)第30条意义上的行政合作组(ADCO)。

委员会可酌情设立其他常设或临时小组，以审查具体问题。在适当情况下，可邀请第67条所述咨询论坛的代表作为观察员参加此类小组或这些小组的特定会议。

7. 委员会的组织和运作应保障其活动的客观性和公正性。

8. 委员会应由成员国代表之一担任主席。人工智能办公室应为委员会提供秘书处，应主席请求召集会议，并根据本条例规定的委员会任务及其议事规则编制议程。

第66条

委员会的任务

委员会应向委员会和成员国提供建议和协助，以促进本条例的一致和有效适用。为此，委员会尤其可以：

(a) 促进负责实施本条例的国家主管机关之间的协调，并与相关市场监督机构合作并在其同意下，支持第74(11)条所述市场监督机构的联合活动；

(b) 在成员国之间收集和分享技术与监管专业知识和最佳实践；

(c) 就本条例的实施提供建议，特别是关于通用人工智能模型规则的执行；

(d) 促进成员国行政实践的统一，包括与第46条所述合格评定程序克减、人工智能监管沙盒的运作以及第57、59和60条所述真实世界条件下测试相关的事项；

(e) 应委员会请求或主动就与本条例实施及其一致有效适用相关的任何有关事项发布建议和书面意见，包括：

(i) 关于依据本条例制定和适用行为准则和业务准则，以及委员会指南；

(ii) 依据第112条对本条例进行评估和审查，包括关于第73条所述严重事件报告、第71条所述欧盟数据库的运作、授权法案或实施法案的准备工作，以及本条例与附件一所列欧盟协调立法可能的协调统一；

(iii) 关于第三章第2节所述要求的技术规范或现有标准；

(iv) on the use of harmonised standards or common specifications referred to in Articles 40 and 41;

(v) trends, such as European global competitiveness in AI, the uptake of AI in the Union, and the development of digital skills;

(vi) trends on the evolving typology of AI value chains, in particular on the resulting implications in terms of accountability;

(vii) on the potential need for amendment to Annex III in accordance with Article 7, and on the potential need for possible revision of Article 5 pursuant to Article 112, taking into account relevant available evidence and the latest developments in technology;

(f) support the Commission in promoting AI literacy, public awareness and understanding of the benefits, risks, safeguards and rights and obligations in relation to the use of AI systems;

(g) facilitate the development of common criteria and a shared understanding among market operators and competent authorities of the relevant concepts provided for in this Regulation, including by contributing to the development of benchmarks;

(h) cooperate, as appropriate, with other Union institutions, bodies, offices and agencies, as well as relevant Union expert groups and networks, in particular in the fields of product safety, cybersecurity, competition, digital and media services, financial services, consumer protection, data and fundamental rights protection;

(i) contribute to effective cooperation with the competent authorities of third countries and with international organisations;

(j) assist national competent authorities and the Commission in developing the organisational and technical expertise required for the implementation of this Regulation, including by contributing to the assessment of training needs for staff of Member States involved in implementing this Regulation;

(k) assist the AI Office in supporting national competent authorities in the establishment and development of AI regulatory sandboxes, and facilitate cooperation and information-sharing among AI regulatory sandboxes;

(l) contribute to, and provide relevant advice on, the development of guidance documents;

(m) advise the Commission in relation to international matters on AI;

(n) provide opinions to the Commission on the qualified alerts regarding general-purpose AI models;

(o) receive opinions by the Member States on qualified alerts regarding general-purpose AI models, and on national experiences and practices on the monitoring and enforcement of AI systems, in particular systems integrating the general-purpose AI models.

Article 67

Advisory forum

1. An advisory forum shall be established to provide technical expertise and advise the Board and the Commission, and to contribute to their tasks under this Regulation.

2. The membership of the advisory forum shall represent a balanced selection of stakeholders, including industry, start-ups, SMEs, civil society and academia. The membership of the advisory forum shall be balanced with regard to commercial and non-commercial interests and, within the category of commercial interests, with regard to SMEs and other undertakings.

3. The Commission shall appoint the members of the advisory forum, in accordance with the criteria set out in paragraph 2, from amongst stakeholders with recognised expertise in the field of AI.

(iv) 关于使用第40条和第41条所述协调标准或通用规范的情况；

(v) 趋势，例如欧洲在人工智能领域的全球竞争力、人工智能在欧盟的采用情况以及数字技能的发展；

(vi) 人工智能价值链类型不断演变的趋势，特别是由此产生的问责方面的影响；

(vii) 关于根据第7条可能需要修订附件III，以及关于根据第112条可能需要修订第5条，同时考虑相关可用证据和技术的最新发展；

(f) 支持委员会促进人工智能素养、公众意识以及对使用人工智能系统的益处、风险、保障措施、权利和义务的理解；

(g) 促进市场运营者和主管机关之间就本条例规定的相关概念制定共同标准并达成共识，包括通过为基准的开发作出贡献；

(h) 酌情与其他欧盟机构、机关、办公室和机构以及相关欧盟专家组和网络合作，特别是在产品安全、网络安全、竞争、数字和媒体服务、金融服务、消费者保护、数据和基本权利保护领域；

(i) 促进与第三国主管当局和国际组织的有效合作；

(j) 协助国家主管机关和委员会发展实施本条例所需的组织和技术专业知识，包括为评估参与实施本条例的成员国工作人员的培训需求作出贡献；

(k) 协助人工智能办公室支持国家主管机关建立和发展人工智能监管沙盒，并促进人工智能监管沙盒之间的合作和信息共享；

(l) 为指南文件的制定做出贡献并提供相关建议；

(m) 就人工智能相关国际事务向委员会提供建议；

(n) 就关于通用人工智能模型的合格警报向委员会提供意见；

(o) 接收成员国就关于通用人工智能模型的合格警报以及就监测和执行人工智能系统(特别是集成通用人工智能模型的系统)方面的国家经验和做法提出的意见。

第67条

咨询论坛

1. 应设立咨询论坛，以提供技术专业知识并向委员会和欧盟委员会提供建议，并为其在本条例下的任务作出贡献。

2. 咨询论坛的成员应代表利益相关方的均衡选择，包括产业界、初创企业、中小企业、民间社会和学术界。咨询论坛的成员应在商业和非商业利益方面保持均衡，在商业利益类别内，应在中小企业和其他企业方面保持均衡。

3. 委员会应根据第2款规定的标准，从在人工智能领域具有公认专业知识的利益相关方中任命咨询论坛的成员。

4. The term of office of the members of the advisory forum shall be two years, which may be extended by up to no more than four years.

5. The Fundamental Rights Agency, ENISA, the European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC), and the European Telecommunications Standards Institute (ETSI) shall be permanent members of the advisory forum.

6. The advisory forum shall draw up its rules of procedure. It shall elect two co-chairs from among its members, in accordance with criteria set out in paragraph 2. The term of office of the co-chairs shall be two years, renewable once.

7. The advisory forum shall hold meetings at least twice a year. The advisory forum may invite experts and other stakeholders to its meetings.

8. The advisory forum may prepare opinions, recommendations and written contributions at the request of the Board or the Commission.

9. The advisory forum may establish standing or temporary sub-groups as appropriate for the purpose of examining specific questions related to the objectives of this Regulation.

10. The advisory forum shall prepare an annual report on its activities. That report shall be made publicly available.

Article 68

Scientific panel of independent experts

1. The Commission shall, by means of an implementing act, make provisions on the establishment of a scientific panel of independent experts (the 'scientific panel') intended to support the enforcement activities under this Regulation. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 98(2).

2. The scientific panel shall consist of experts selected by the Commission on the basis of up-to-date scientific or technical expertise in the field of AI necessary for the tasks set out in paragraph 3, and shall be able to demonstrate meeting all of the following conditions:

(a) having particular expertise and competence and scientific or technical expertise in the field of AI;

(b) independence from any provider of AI systems or general-purpose AI models;

(c) an ability to carry out activities diligently, accurately and objectively.

The Commission, in consultation with the Board, shall determine the number of experts on the panel in accordance with the required needs and shall ensure fair gender and geographical representation.

3. The scientific panel shall advise and support the AI Office, in particular with regard to the following tasks:

(a) supporting the implementation and enforcement of this Regulation as regards general-purpose AI models and systems, in particular by:

(i) alerting the AI Office of possible systemic risks at Union level of general-purpose AI models, in accordance with Article 90;

(ii) contributing to the development of tools and methodologies for evaluating capabilities of general-purpose AI models and systems, including through benchmarks;

(iii) providing advice on the classification of general-purpose AI models with systemic risk;

(iv) providing advice on the classification of various general-purpose AI models and systems;

4. 咨询论坛成员的任期为两年，可延长不超过四年。

5. 基本权利机构、ENISA、欧洲标准化委员会(CEN)、欧洲电工标准化委员会(CENELEC)和欧洲电信标准协会(ETSI)应为咨询论坛的常任成员。

6. 咨询论坛应制定其议事规则。应根据第2款规定的标准，从其成员中选举两名联合主席。联合主席的任期为两年，可连任一次。

7. 咨询论坛应每年至少举行两次会议。咨询论坛可邀请专家和其他利益相关方参加其会议。

8. 咨询论坛可应委员会或欧盟委员会的要求编写意见、建议和书面文稿。

9. 咨询论坛可酌情设立常设或临时分组，以审查与本条例目标相关的具体问题。

10. 咨询论坛应编写关于其活动的年度报告。该报告应公开提供。

第68条

独立专家科学小组

1. 委员会应通过实施法案，就设立一个旨在支持本条例下执法活动的独立专家科学小组("科学小组")作出规定。该实施法案应根据第98条第2款所述审查程序通过。

2. 科学小组应由委员会根据人工智能领域最新的科学或技术专业知识选出的专家组成，这些专业知识是第3款所述任务所必需的，并应能够证明满足以下所有条件：

(a) 在人工智能领域具有特定的专业知识和能力以及科学或技术专业知识；

(b) 独立于任何AI系统或通用目的AI模型的提供者；

(c) 勤勉、准确和客观地开展活动的能力。

委员会应与理事会协商，根据所需确定小组专家人数，并应确保公平的性别和地域代表性。

3. 科学小组应向人工智能办公室提供建议和支持，特别是在以下任务方面：

(a) 支持本条例在通用人工智能模型和系统方面的实施和执法，特别是通过：

(i) 根据第90条，就通用人工智能模型在欧盟层面可能存在的系统性风险向人工智能办公室发出警报；

(ii) 为开发评估通用人工智能模型和系统能力的工具和方法作出贡献，包括通过基准；

(iii) 就具有系统性风险的通用人工智能模型的分类提供建议；

(iv) 就各类通用人工智能模型和系统的分类提供建议；

(v) contributing to the development of tools and templates;

(b) supporting the work of market surveillance authorities, at their request;

(c) supporting cross-border market surveillance activities as referred to in Article 74(11), without prejudice to the powers of market surveillance authorities;

(d) supporting the AI Office in carrying out its duties in the context of the Union safeguard procedure pursuant to Article 81.

4. The experts on the scientific panel shall perform their tasks with impartiality and objectivity, and shall ensure the confidentiality of information and data obtained in carrying out their tasks and activities. They shall neither seek nor take instructions from anyone when exercising their tasks under paragraph 3. Each expert shall draw up a declaration of interests, which shall be made publicly available. The AI Office shall establish systems and procedures to actively manage and prevent potential conflicts of interest.

5. The implementing act referred to in paragraph 1 shall include provisions on the conditions, procedures and detailed arrangements for the scientific panel and its members to issue alerts, and to request the assistance of the AI Office for the performance of the tasks of the scientific panel.

Article 69

Access to the pool of experts by the Member States

1. Member States may call upon experts of the scientific panel to support their enforcement activities under this Regulation.

2. The Member States may be required to pay fees for the advice and support provided by the experts. The structure and the level of fees as well as the scale and structure of recoverable costs shall be set out in the implementing act referred to in Article 68(1), taking into account the objectives of the adequate implementation of this Regulation, cost-effectiveness and the necessity of ensuring effective access to experts for all Member States.

3. The Commission shall facilitate timely access to the experts by the Member States, as needed, and ensure that the combination of support activities carried out by Union AI testing support pursuant to Article 84 and experts pursuant to this Article is efficiently organised and provides the best possible added value.

SECTION 2

National competent authorities

Article 70

Designation of national competent authorities and single points of contact

1. Each Member State shall establish or designate as national competent authorities at least one notifying authority and at least one market surveillance authority for the purposes of this Regulation. Those national competent authorities shall exercise their powers independently, impartially and without bias so as to safeguard the objectivity of their activities and tasks, and to ensure the application and implementation of this Regulation. The members of those authorities shall refrain from any action incompatible with their duties. Provided that those principles are observed, such activities and tasks may be performed by one or more designated authorities, in accordance with the organisational needs of the Member State.

2. Member States shall communicate to the Commission the identity of the notifying authorities and the market surveillance authorities and the tasks of those authorities, as well as any subsequent changes thereto. Member States shall make publicly available information on how competent authorities and single points of contact can be contacted, through electronic communication means by 2 August 2025. Member States shall designate a market surveillance authority to act as the single point of contact for this Regulation, and shall notify the Commission of the identity of the single point of contact. The Commission shall make a list of the single points of contact publicly available.

(v) 协助开发工具和模板；

(b) 应市场监督机构请求，支持其工作；

(c) 在不影响市场监督机构权力的前提下，支持第74(11)条所述跨境市场监督活动；

(d) 支持人工智能办公室履行第81条所述欧盟保障程序中的职责。

4. 科学小组的专家应当公正、客观地履行职责，并应当确保对在履行其任务和活动过程中获得的信息和数据保密。专家在根据第3款行使任务时，不得寻求或接受任何人的指示。每位专家应当拟定一份利益声明，该声明应当予以公开。人工智能办公室应当建立系统和程序，以积极管理和防止潜在的利益冲突。

5. 第1款所述实施法案应包括关于科学小组及其成员发出警报以及请求人工智能办公室协助履行科学小组任务的条件、程序和详细安排的规定。

第69条

成员国对专家库的访问

1. 成员国可邀请科学小组的专家支持其根据本条例开展的执法活动。

2. 成员国可能被要求为专家提供的建议和支持支付费用。费用的结构和水平以及可收回费用的规模和结构应在第68(1)条所述实施法案中规定，同时考虑充分实施本条例的目标、成本效益以及确保所有成员国有效获得专家支持的必要性。

3. 委员会应促进成员国在需要时及时获得专家支持，并确保根据第84条由欧盟人工智能测试支持开展的支持活动与本条所述专家支持活动的组合得到高效组织，并提供尽可能最佳的附加值。

第2节

国家主管机关

第70条

国家主管机关和单一联系点的指定

1. 每个成员国应当为本条例的目的设立或指定至少一个通知机构和至少一个市场监督机构作为国家主管机关。这些国家主管机关应当独立、公正、无偏见地行使其权力，以保障其活动和任务的客观性，并确保本条例的适用和实施。这些机关的成员应当避免任何与其职责不相容的行为。在遵守这些原则的前提下，根据成员国的组织需要，此类活动和任务可由一个或多个指定机关执行。

2. 成员国应向委员会通报通知机构和市场监督机构的身份及这些机构的任务，以及其后任何变更。成员国应在2025年8月2日前通过电子通信方式公开关于如何联系主管机关和单一联络点的信息。成员国应指定一个市场监督机构作为本条例的单一联络点，并应将单一联络点的身份通知委员会。委员会应公开单一联络点清单。

3. Member States shall ensure that their national competent authorities are provided with adequate technical, financial and human resources, and with infrastructure to fulfil their tasks effectively under this Regulation. In particular, the national competent authorities shall have a sufficient number of personnel permanently available whose competences and expertise shall include an in-depth understanding of AI technologies, data and data computing, personal data protection, cybersecurity, fundamental rights, health and safety risks and knowledge of existing standards and legal requirements. Member States shall assess and, if necessary, update competence and resource requirements referred to in this paragraph on an annual basis.

4. National competent authorities shall take appropriate measures to ensure an adequate level of cybersecurity.

5. When performing their tasks, the national competent authorities shall act in accordance with the confidentiality obligations set out in Article 78.

6. By 2 August 2025, and once every two years thereafter, Member States shall report to the Commission on the status of the financial and human resources of the national competent authorities, with an assessment of their adequacy. The Commission shall transmit that information to the Board for discussion and possible recommendations.

7. The Commission shall facilitate the exchange of experience between national competent authorities.

8. National competent authorities may provide guidance and advice on the implementation of this Regulation, in particular to SMEs including start-ups, taking into account the guidance and advice of the Board and the Commission, as appropriate. Whenever national competent authorities intend to provide guidance and advice with regard to an AI system in areas covered by other Union law, the national competent authorities under that Union law shall be consulted, as appropriate.

9. Where Union institutions, bodies, offices or agencies fall within the scope of this Regulation, the European Data Protection Supervisor shall act as the competent authority for their supervision.

CHAPTER VIII

EU DATABASE FOR HIGH-RISK AI SYSTEMS

Article 71

EU database for high-risk AI systems listed in Annex III

1. The Commission shall, in collaboration with the Member States, set up and maintain an EU database containing information referred to in paragraphs 2 and 3 of this Article concerning high-risk AI systems referred to in Article 6(2) which are registered in accordance with Articles 49 and 60 and AI systems that are not considered as high-risk pursuant to Article 6(3) and which are registered in accordance with Article 6(4) and Article 49. When setting the functional specifications of such database, the Commission shall consult the relevant experts, and when updating the functional specifications of such database, the Commission shall consult the Board.

2. The data listed in Sections A and B of Annex VIII shall be entered into the EU database by the provider or, where applicable, by the authorised representative.

3. The data listed in Section C of Annex VIII shall be entered into the EU database by the deployer who is, or who acts on behalf of, a public authority, agency or body, in accordance with Article 49(3) and (4).

4. With the exception of the section referred to in Article 49(4) and Article 60(4), point (c), the information contained in the EU database registered in accordance with Article 49 shall be accessible and publicly available in a user-friendly manner. The information should be easily navigable and machine-readable. The information registered in accordance with Article 60 shall be accessible only to market surveillance authorities and the Commission, unless the prospective provider or provider has given consent for also making the information accessible the public.

5. The EU database shall contain personal data only in so far as necessary for collecting and processing information in accordance with this Regulation. That information shall include the names and contact details of natural persons who are responsible for registering the system and have the legal authority to represent the provider or the deployer, as applicable.

3. 成员国应当确保其国家主管机关获得充足的技术、财政和人力资源以及基础设施，以有效履行本条例规定的任务。特别是，国家主管机关应当拥有足够数量的长期可用人员，其能力和专业知识应当包括对人工智能技术、数据和数据计算、个人数据保护、网络安全、基本权利、健康和安全风险以及现有标准法律要求的深入了解。成员国应当每年评估并在必要时更新本款所述的能力和资源要求。

4. 国家主管机关应采取适当措施确保适当的网络安全水平。

5. 国家主管机关在履行职责时应遵守第78条规定的保密义务。

6. 到2025年8月2日，此后每两年一次，成员国应向委员会报告国家主管机关的财政和人力资源状况，并附对其充分性的评估。委员会应将该信息转交委员会(Board)供讨论并可能提出建议。

7. 委员会应促进国家主管机关之间的经验交流。

8. 国家主管机关可酌情考虑委员会(理事会)和委员会的指导和建议，就本条例的实施提供指导和建议，特别是向中小企业包括初创企业提供指导和建议。当国家主管机关打算就其他欧盟法律所涵盖领域的人工智能系统提供指导和建议时，应酌情咨询该欧盟法律下的国家主管机关。

9. 当欧盟机构、机关、办公室或机构属于本条例范围时，欧洲数据保护监督员应作为其监督的主管机关。

第八章

高风险 AI 系统欧盟数据库

第71条

附件三所列高风险人工智能系统的欧盟数据库

1. 委员会应当与成员国合作，建立并维护一个欧盟数据库，其中包含本条第2款和第3款所述关于第6(2)条所述高风险人工智能系统的信息，这些系统根据第49条和第60条进行登记，以及根据第6(3)条不被视为高风险且根据第6(4)条和第49条进行登记的人工智能系统的信息。在设定此类数据库的功能规范时，委员会应当咨询相关专家，在更新此类数据库的功能规范时，委员会应当咨询委员会。

2. 附件VIII A节和B节所列数据应由提供者或酌情由授权代表录入欧盟数据库。

3. 附件VIII C节所列数据应由作为公共机构、机关或团体或代表其行事的部署者根据第49(3)条和第49(4)条录入欧盟数据库。

4. 除Article 49(4)和Article 60(4) point (c)所述部分外，依照Article 49注册的EU数据库中包含的信息应以用户友好的方式可访问并向公众公开。该信息应易于浏览且机器可读。依照Article 60注册的信息仅应由市场监督机构和委员会访问，除非潜在提供者或提供者已同意将该信息也向公众公开。

5. 欧盟数据库仅应在根据本条例收集和处理信息所必要的范围内包含个人数据。该信息应包括负责注册系统并具有代表提供者或部署者(视情况而定)法定权限的自然人的姓名和联系方式。

6. The Commission shall be the controller of the EU database. It shall make available to providers, prospective providers and deployers adequate technical and administrative support. The EU database shall comply with the applicable accessibility requirements.

CHAPTER IX

POST-MARKET MONITORING, INFORMATION SHARING AND MARKET SURVEILLANCE

SECTION 1

Post-market monitoring

Article 72

Post-market monitoring by providers and post-market monitoring plan for high-risk AI systems

1. Providers shall establish and document a post-market monitoring system in a manner that is proportionate to the nature of the AI technologies and the risks of the high-risk AI system.

2. The post-market monitoring system shall actively and systematically collect, document and analyse relevant data which may be provided by deployers or which may be collected through other sources on the performance of high-risk AI systems throughout their lifetime, and which allow the provider to evaluate the continuous compliance of AI systems with the requirements set out in Chapter III, Section 2. Where relevant, post-market monitoring shall include an analysis of the interaction with other AI systems. This obligation shall not cover sensitive operational data of deployers which are law-enforcement authorities.

3. The post-market monitoring system shall be based on a post-market monitoring plan. The post-market monitoring plan shall be part of the technical documentation referred to in Annex IV. The Commission shall adopt an implementing act laying down detailed provisions establishing a template for the post-market monitoring plan and the list of elements to be included in the plan by 2 February 2026. That implementing act shall be adopted in accordance with the examination procedure referred to in Article 98(2).

4. For high-risk AI systems covered by the Union harmonisation legislation listed in Section A of Annex I, where a post-market monitoring system and plan are already established under that legislation, in order to ensure consistency, avoid duplications and minimise additional burdens, providers shall have a choice of integrating, as appropriate, the necessary elements described in paragraphs 1, 2 and 3 using the template referred in paragraph 3 into systems and plans already existing under that legislation, provided that it achieves an equivalent level of protection.

The first subparagraph of this paragraph shall also apply to high-risk AI systems referred to in point 5 of Annex III placed on the market or put into service by financial institutions that are subject to requirements under Union financial services law regarding their internal governance, arrangements or processes.

SECTION 2

Sharing of information on serious incidents

Article 73

Reporting of serious incidents

1. Providers of high-risk AI systems placed on the Union market shall report any serious incident to the market surveillance authorities of the Member States where that incident occurred.

6. 委员会应作为欧盟数据库的控制者。其应向提供者、潜在提供者和部署者提供适当的技术和行政支持。欧盟数据库应符合适用的无障碍要求。

第九章

投放市场后监测、信息共享和市场监督

第1节

上市后监测

第72条

提供者的上市后监测和高风险人工智能系统的上市后监测计划

1. 提供者应以与人工智能技术的性质和高风险人工智能系统的风险相称的方式建立并记录上市后监测系统。

2. 上市后监测系统应主动、系统地收集、记录和分析相关数据，这些数据可能由部署者提供，或可能通过其他来源收集，涉及高风险人工智能系统在其整个生命周期内的性能，并使提供者能够评估人工智能系统对Chapter III, Section 2所规定要求的持续合规性。在相关情况下，上市后监测应包括对其他人工智能系统交互的分析。该义务不应涵盖属于执法机构的部署者的敏感操作数据。

3. 上市后监测系统应基于上市后监测计划。上市后监测计划应构成Annex IV所述技术文档的一部分。委员会应在2 August 2026之前通过一项实施法案，规定详细条款，确立上市后监测计划的模板以及该计划应包含的要素清单。该实施法案应依照Article 98(2)所述审查程序通过。

4. 对于Annex I Section A所列欧盟协调立法所涵盖的高风险人工智能系统，若已根据该立法建立了上市后监测系统和计划，为确保一致性、避免重复并尽量减少额外负担，提供者应有权选择酌情使用paragraph 3所述模板，将paragraphs 1、2和3所述必要要素整合到该立法下已存在的系统和计划中，前提是达到同等保护水平。

本款第一项亦适用于由受欧盟金融服务法关于其内部治理、安排或程序要求约束的金融机构投放市场或投入使用的附件三第5点所述高风险人工智能系统。

第2节

严重事件信息的共享

第73条

严重事件报告

1. 在欧盟市场投放高风险人工智能系统的提供者应向事件发生成员国的市场监督机构报告任何严重事件。

2. The report referred to in paragraph 1 shall be made immediately after the provider has established a causal link between the AI system and the serious incident or the reasonable likelihood of such a link, and, in any event, not later than 15 days after the provider or, where applicable, the deployer, becomes aware of the serious incident.

The period for the reporting referred to in the first subparagraph shall take account of the severity of the serious incident.

3. Notwithstanding paragraph 2 of this Article, in the event of a widespread infringement or a serious incident as defined in Article 3, point (49)(b), the report referred to in paragraph 1 of this Article shall be provided immediately, and not later than two days after the provider or, where applicable, the deployer becomes aware of that incident.

4. Notwithstanding paragraph 2, in the event of the death of a person, the report shall be provided immediately after the provider or the deployer has established, or as soon as it suspects, a causal relationship between the high-risk AI system and the serious incident, but not later than 10 days after the date on which the provider or, where applicable, the deployer becomes aware of the serious incident.

5. Where necessary to ensure timely reporting, the provider or, where applicable, the deployer, may submit an initial report that is incomplete, followed by a complete report.

6. Following the reporting of a serious incident pursuant to paragraph 1, the provider shall, without delay, perform the necessary investigations in relation to the serious incident and the AI system concerned. This shall include a risk assessment of the incident, and corrective action.

The provider shall cooperate with the competent authorities, and where relevant with the notified body concerned, during the investigations referred to in the first subparagraph, and shall not perform any investigation which involves altering the AI system concerned in a way which may affect any subsequent evaluation of the causes of the incident, prior to informing the competent authorities of such action.

7. Upon receiving a notification related to a serious incident referred to in Article 3, point (49)(c), the relevant market surveillance authority shall inform the national public authorities or bodies referred to in Article 77(1). The Commission shall develop dedicated guidance to facilitate compliance with the obligations set out in paragraph 1 of this Article. That guidance shall be issued by 2 August 2025, and shall be assessed regularly.

8. The market surveillance authority shall take appropriate measures, as provided for in Article 19 of Regulation (EU) 2019/1020, within seven days from the date it received the notification referred to in paragraph 1 of this Article, and shall follow the notification procedures as provided in that Regulation.

9. For high-risk AI systems referred to in Annex III that are placed on the market or put into service by providers that are subject to Union legislative instruments laying down reporting obligations equivalent to those set out in this Regulation, the notification of serious incidents shall be limited to those referred to in Article 3, point (49)(c).

10. For high-risk AI systems which are safety components of devices, or are themselves devices, covered by Regulations (EU) 2017/745 and (EU) 2017/746, the notification of serious incidents shall be limited to those referred to in Article 3, point (49)(c) of this Regulation, and shall be made to the national competent authority chosen for that purpose by the Member States where the incident occurred.

11. National competent authorities shall immediately notify the Commission of any serious incident, whether or not they have taken action on it, in accordance with Article 20 of Regulation (EU) 2019/1020.

SECTION 3

Enforcement

Article 74

Market surveillance and control of AI systems in the Union market

1. Regulation (EU) 2019/1020 shall apply to AI systems covered by this Regulation. For the purposes of the effective enforcement of this Regulation:

2. 第1款所述报告应在提供者确定人工智能系统与严重事件之间的因果关系或此类联系存在合理可能性后立即提交，且在任何情况下不得迟于提供者或酌情部署者知悉严重事件后15天。

第一项所指的报告期限应考虑严重事件的严重程度。

3. 尽管有本条第2款的规定，在发生第3条第(49)项(b)目所定义的广泛侵权或严重事件时，本条第1款所述报告应立即提供，且不得迟于提供者或酌情部署者知悉该事件后两天。

4. 尽管有第2款的规定，在发生人员死亡的情况下，报告应在提供者或部署者确定或一旦怀疑高风险人工智能系统与严重事件之间存在因果关系后立即提供，但不得迟于提供者或酌情部署者知悉严重事件之日起10天。

5. 为确保及时报告，提供者或酌情部署者可提交不完整的初步报告，随后提交完整报告。

6. 在根据第1款报告严重事件后，提供者应立即对严重事件和相关人工智能系统进行必要的调查。这应包括对事件的风险评估和纠正措施。

提供者应在第一项所述调查期间与主管机关合作，并在相关情况下与相关公告机构合作，且在告知主管机关此类行动之前，不得进行任何涉及以可能影响对事件原因任何后续评估的方式更改相关人工智能系统的调查。

7. 收到与第3条第(49)款(c)项所述严重事件相关的通知后，相关市场监督机构应告知第77(1)条所述的国家公共机构或机关。委员会应制定专门指南，以促进对本条第1款所规定义务的遵守。该指南应于2025年8月2日前发布，并应定期评估。

8. 市场监督机构应按照(欧盟)2019/1020号条例第19条的规定，在收到本条第1款所述通知之日起七天内采取适当措施，并应遵循该条例规定的通知程序。

9. 对于附件III所述由受欧盟立法文书约束且该文书规定了与本条例规定等效的报告义务的提供者投放市场或投入服务的高风险人工智能系统，严重事件的通知应限于第3条第(49)项(c)目所述事件。

10. 对于作为(欧盟)2017/745号条例和(欧盟)2017/746号条例所涵盖器械的安全组件的高风险人工智能系统，或本身即为该类器械的高风险人工智能系统，严重事件的通知应限于本条例第3条第(49)项(c)目所述事件，并应向事件发生成员国为此目的选定的国家主管机关提交。

11. 国家主管机关应根据Regulation(EU) 2019/1020第20条，立即将任何严重事件通知委员会，无论其是否已对该事件采取行动。

第3节

执法

第74条

欧盟市场中人工智能系统的市场监督与控制

1. (EU) 2019/1020号条例应适用于本条例所涵盖的人工智能系统。为有效执行本条例：

(a) any reference to an economic operator under Regulation (EU) 2019/1020 shall be understood as including all operators identified in Article 2(1) of this Regulation;

(b) any reference to a product under Regulation (EU) 2019/1020 shall be understood as including all AI systems falling within the scope of this Regulation.

2. As part of their reporting obligations under Article 34(4) of Regulation (EU) 2019/1020, the market surveillance authorities shall report annually to the Commission and relevant national competition authorities any information identified in the course of market surveillance activities that may be of potential interest for the application of Union law on competition rules. They shall also annually report to the Commission about the use of prohibited practices that occurred during that year and about the measures taken.

3. For high-risk AI systems related to products covered by the Union harmonisation legislation listed in Section A of Annex I, the market surveillance authority for the purposes of this Regulation shall be the authority responsible for market surveillance activities designated under those legal acts.

By derogation from the first subparagraph, and in appropriate circumstances, Member States may designate another relevant authority to act as a market surveillance authority, provided they ensure coordination with the relevant sectoral market surveillance authorities responsible for the enforcement of the Union harmonisation legislation listed in Annex I.

4. The procedures referred to in Articles 79 to 83 of this Regulation shall not apply to AI systems related to products covered by the Union harmonisation legislation listed in section A of Annex I, where such legal acts already provide for procedures ensuring an equivalent level of protection and having the same objective. In such cases, the relevant sectoral procedures shall apply instead.

5. Without prejudice to the powers of market surveillance authorities under Article 14 of Regulation (EU) 2019/1020, for the purpose of ensuring the effective enforcement of this Regulation, market surveillance authorities may exercise the powers referred to in Article 14(4), points (d) and (j), of that Regulation remotely, as appropriate.

6. For high-risk AI systems placed on the market, put into service, or used by financial institutions regulated by Union financial services law, the market surveillance authority for the purposes of this Regulation shall be the relevant national authority responsible for the financial supervision of those institutions under that legislation in so far as the placing on the market, putting into service, or the use of the AI system is in direct connection with the provision of those financial services.

7. By way of derogation from paragraph 6, in appropriate circumstances, and provided that coordination is ensured, another relevant authority may be identified by the Member State as market surveillance authority for the purposes of this Regulation.

National market surveillance authorities supervising regulated credit institutions regulated under Directive 2013/36/EU, which are participating in the Single Supervisory Mechanism established by Regulation (EU) No 1024/2013, should report, without delay, to the European Central Bank any information identified in the course of their market surveillance activities that may be of potential interest for the prudential supervisory tasks of the European Central Bank specified in that Regulation.

8. For high-risk AI systems listed in point 1 of Annex III to this Regulation, in so far as the systems are used for law enforcement purposes, border management and justice and democracy, and for high-risk AI systems listed in points 6, 7 and 8 of Annex III to this Regulation, Member States shall designate as market surveillance authorities for the purposes of this Regulation either the competent data protection supervisory authorities under Regulation (EU) 2016/679 or Directive (EU) 2016/680, or any other authority designated pursuant to the same conditions laid down in Articles 41 to 44 of Directive (EU) 2016/680. Market surveillance activities shall in no way affect the independence of judicial authorities, or otherwise interfere with their activities when acting in their judicial capacity.

9. Where Union institutions, bodies, offices or agencies fall within the scope of this Regulation, the European Data Protection Supervisor shall act as their market surveillance authority, except in relation to the Court of Justice of the European Union acting in its judicial capacity.

10. Member States shall facilitate coordination between market surveillance authorities designated under this Regulation and other relevant national authorities or bodies which supervise the application of Union harmonisation legislation listed in Annex I, or in other Union law, that might be relevant for the high-risk AI systems referred to in Annex III.

(a) (EU) 2019/1020号条例中任何对经济运营者的引用应理解为包括本条例第2(1)条所识别的所有运营者；

(b) (EU) 2019/1020号条例中任何对产品的引用应理解为包括属于本条例范围内的所有人工智能系统。

2. 作为Regulation (EU) 2019/1020 Article 34(4)下报告义务的一部分，市场监督机构应每年向委员会和相关国家竞争主管机构报告在市场监督活动中发现的、可能对欧盟竞争规则适用具有潜在利益的任何信息。它们还应每年向委员会报告该年度内发生的禁止性实践的使用情况以及所采取的措施。

3. 对于与附件I A节所列欧盟协调立法所涵盖产品相关的高风险人工智能系统，就本条例而言，市场监督机构应为根据这些法律法案指定的负责市场监督活动的机构。

作为对第一款的减损，在适当情况下，成员国可指定另一相关机构作为市场监督机构，前提是其确保与负责执行附件I所列欧盟协调立法的相关行业市场监督机构进行协调。

4. 本条例第79至83条所述程序不适用于与附件I A节所列欧盟协调立法所涵盖产品相关的人工智能系统，前提是此类法律法案已规定了确保同等保护水平且具有相同目标的程序。在此类情况下，应改为适用相关行业程序。

5. 在不影响市场监督机构根据(EU) 2019/1020号条例第14条所享有权力的情况下，为确保本条例的有效执行，市场监督机构可酌情远程行使该条例第14(4)条(d)项和(j)项所述权力。

6. 对于由欧盟金融服务法律监管的金融机构投放市场、投入使用或使用的高风险人工智能系统，就本条例而言，市场监督机构应为根据该法律负责对这些机构进行金融监管的相关国家主管机构，前提是该人工智能系统的投放市场、投入使用或使用与提供这些金融服务直接相关。

7. 作为对第6款的减损，在适当情况下，并在确保协调的前提下，成员国可确定另一相关机构作为本条例目的下的市场监督机构。

监督受指令2013/36/EU监管的受监管信贷机构(该等机构参与根据欧盟条例(EU) 第1024/2013号建立的单一监督机制)的国家市场监督机构，应毫不迟延地向欧洲中央银行报告其在市场监督活动中发现的、可能对该条例规定的欧洲中央银行审慎监管任务具有潜在利益的任何信息。

8. 对于本条例附件三第1点所列的高风险人工智能系统，只要这些系统用于执法、边境管理以及司法与民主目的，以及对于本条例附件三第6点、第7点和第8点所列的高风险人工智能系统，成员国应指定根据条例(EU) 2016/679或指令(EU) 2016/680设立的主管数据保护监督机构，或根据指令(EU) 2016/680第41条至第44条规定的相同条件指定的任何其他机构，作为本条例目的下的市场监督机构。市场监督活动不得以任何方式影响司法机关的独立性，也不得在其以司法身份行事时干扰其活动。

9. 当欧盟机构、机关、办事处或团体属于本条例范围时，欧洲数据保护监督员应作为其市场监督机构，但欧洲联盟法院以司法身份行事的情况除外。

10. 成员国应促进根据本条例指定的市场监督机构与监督附件I所列欧盟协调立法或其他可能对附件III所述高风险人工智能系统相关的欧盟法律适用情况的其他相关国家主管机关或机构之间的协调。

11. Market surveillance authorities and the Commission shall be able to propose joint activities, including joint investigations, to be conducted by either market surveillance authorities or market surveillance authorities jointly with the Commission, that have the aim of promoting compliance, identifying non-compliance, raising awareness or providing guidance in relation to this Regulation with respect to specific categories of high-risk AI systems that are found to present a serious risk across two or more Member States in accordance with Article 9 of Regulation (EU) 2019/1020. The AI Office shall provide coordination support for joint investigations.

12. Without prejudice to the powers provided for under Regulation (EU) 2019/1020, and where relevant and limited to what is necessary to fulfil their tasks, the market surveillance authorities shall be granted full access by providers to the documentation as well as the training, validation and testing data sets used for the development of high-risk AI systems, including, where appropriate and subject to security safeguards, through application programming interfaces (API) or other relevant technical means and tools enabling remote access.

13. Market surveillance authorities shall be granted access to the source code of the high-risk AI system upon a reasoned request and only when both of the following conditions are fulfilled:

(a) access to source code is necessary to assess the conformity of a high-risk AI system with the requirements set out in Chapter III, Section 2; and

(b) testing or auditing procedures and verifications based on the data and documentation provided by the provider have been exhausted or proved insufficient.

14. Any information or documentation obtained by market surveillance authorities shall be treated in accordance with the confidentiality obligations set out in Article 78.

Article 75

Mutual assistance, market surveillance and control of general-purpose AI systems

1. Where an AI system is based on a general-purpose AI model, and the model and the system are developed by the same provider, the AI Office shall have powers to monitor and supervise compliance of that AI system with obligations under this Regulation. To carry out its monitoring and supervision tasks, the AI Office shall have all the powers of a market surveillance authority provided for in this Section and Regulation (EU) 2019/1020.

2. Where the relevant market surveillance authorities have sufficient reason to consider general-purpose AI systems that can be used directly by deployers for at least one purpose that is classified as high-risk pursuant to this Regulation to be non-compliant with the requirements laid down in this Regulation, they shall cooperate with the AI Office to carry out compliance evaluations, and shall inform the Board and other market surveillance authorities accordingly.

3. Where a market surveillance authority is unable to conclude its investigation of the high-risk AI system because of its inability to access certain information related to the general-purpose AI model despite having made all appropriate efforts to obtain that information, it may submit a reasoned request to the AI Office, by which access to that information shall be enforced. In that case, the AI Office shall supply to the applicant authority without delay, and in any event within 30 days, any information that the AI Office considers to be relevant in order to establish whether a high-risk AI system is non-compliant. Market surveillance authorities shall safeguard the confidentiality of the information that they obtain in accordance with Article 78 of this Regulation. The procedure provided for in Chapter VI of Regulation (EU) 2019/1020 shall apply *mutatis mutandis*.

Article 76

Supervision of testing in real world conditions by market surveillance authorities

1. Market surveillance authorities shall have competences and powers to ensure that testing in real world conditions is in accordance with this Regulation.

11. 市场监督机构和委员会应能够提议开展联合活动，包括由市场监督机构或市场监督机构与委员会联合开展的联合调查，其目的是根据条例(EU) 2019/1020第9条，针对被发现对两个或以上成员国构成严重风险的特定类别高风险人工智能系统，促进合规、识别不合规行为、提高认识或提供与本条例相关的指导。人工智能办公室应为联合调查提供协调支持。

12. 在不影响条例(EU) 2019/1020所规定权力的情况下，并在相关且限于完成任务所必需的范围内，提供者应授予市场监督机构对用于开发高风险人工智能系统的文档以及训练、验证和测试数据集的完全访问权限，包括在适当情况下并在符合安全保障措施的前提下，通过应用程序编程接口(API)或其他能够实现远程访问的相关技术手段和工具进行访问。

13. 市场监督机构应经合理请求获得高风险人工智能系统的源代码，且仅在以下两个条件均满足时：

(a) 访问源代码对于评估高风险人工智能系统是否符合第三章第2节规定的要求是必要的；且

(b) 基于提供者所提供数据和文件的测试或审计程序及验证已用尽或被证明不充分。

14. 市场监督机构获得的任何信息或文件应按照第78条规定的保密义务处理。

第75条

通用人工智能系统的互助、市场监督和控制

1. 当人工智能系统基于通用人工智能模型，且该模型和系统由同一提供者开发时，人工智能办公室应有权监督和监管该人工智能系统对本条例义务的遵守情况。为执行其监督和监管任务，人工智能办公室应享有本节和(EU) 2019/1020号条例规定的市场监督机构的全部权力。

2. 当相关市场监督机构有充分理由认为，可由部署者直接用于至少一个根据本条例被归类为高风险目的的通用人工智能系统不符合本条例规定的要求时，其应与人工智能办公室合作进行合规评估，并相应通知委员会和其他市场监督机构。

3. 如果市场监督机构因无法访问与通用人工智能模型相关的某些信息而无法完成对高风险人工智能系统的调查，尽管已作出一切适当努力获取该信息，其可向人工智能办公室提交附有理由的请求，据此应强制授予对该信息的访问权限。在此情况下，人工智能办公室应毫不迟延地向申请机构提供其认为对确定高风险人工智能系统是否不合规具有相关性的任何信息，且在任何情况下应在30天内提供。市场监督机构应根据本条例第78条保障其获得的信息的机密性。条例(EU) 2019/1020第六章规定的程序应比照适用。

第76条

市场监督机构对真实世界条件下测试的监督

1. 市场监督机构应具备确保真实世界条件下测试符合本条例的职权和权力。

2. Where testing in real world conditions is conducted for AI systems that are supervised within an AI regulatory sandbox under Article 58, the market surveillance authorities shall verify the compliance with Article 60 as part of their supervisory role for the AI regulatory sandbox. Those authorities may, as appropriate, allow the testing in real world conditions to be conducted by the provider or prospective provider, in derogation from the conditions set out in Article 60(4), points (f) and (g).

3. Where a market surveillance authority has been informed by the prospective provider, the provider or any third party of a serious incident or has other grounds for considering that the conditions set out in Articles 60 and 61 are not met, it may take either of the following decisions on its territory, as appropriate:

(a) to suspend or terminate the testing in real world conditions;

(b) to require the provider or prospective provider and the deployer or prospective deployer to modify any aspect of the testing in real world conditions.

4. Where a market surveillance authority has taken a decision referred to in paragraph 3 of this Article, or has issued an objection within the meaning of Article 60(4), point (b), the decision or the objection shall indicate the grounds therefor and how the provider or prospective provider can challenge the decision or objection.

5. Where applicable, where a market surveillance authority has taken a decision referred to in paragraph 3, it shall communicate the grounds therefor to the market surveillance authorities of other Member States in which the AI system has been tested in accordance with the testing plan.

Article 77

Powers of authorities protecting fundamental rights

1. National public authorities or bodies which supervise or enforce the respect of obligations under Union law protecting fundamental rights, including the right to non-discrimination, in relation to the use of high-risk AI systems referred to in Annex III shall have the power to request and access any documentation created or maintained under this Regulation in accessible language and format when access to that documentation is necessary for effectively fulfilling their mandates within the limits of their jurisdiction. The relevant public authority or body shall inform the market surveillance authority of the Member State concerned of any such request.

2. By 2 November 2024, each Member State shall identify the public authorities or bodies referred to in paragraph 1 and make a list of them publicly available. Member States shall notify the list to the Commission and to the other Member States, and shall keep the list up to date.

3. Where the documentation referred to in paragraph 1 is insufficient to ascertain whether an infringement of obligations under Union law protecting fundamental rights has occurred, the public authority or body referred to in paragraph 1 may make a reasoned request to the market surveillance authority, to organise testing of the high-risk AI system through technical means. The market surveillance authority shall organise the testing with the close involvement of the requesting public authority or body within a reasonable time following the request.

4. Any information or documentation obtained by the national public authorities or bodies referred to in paragraph 1 of this Article pursuant to this Article shall be treated in accordance with the confidentiality obligations set out in Article 78.

Article 78

Confidentiality

1. The Commission, market surveillance authorities and notified bodies and any other natural or legal person involved in the application of this Regulation shall, in accordance with Union or national law, respect the confidentiality of information and data obtained in carrying out their tasks and activities in such a manner as to protect, in particular:

2. 对于在根据Article 58设立的人工智能监管沙盒内接受监督的人工智能系统，若在真实世界条件下进行测试，市场监督机构应作为其对人工智能监管沙盒监督职责的一部分，核实其是否符合Article 60的规定。这些机构可酌情允许提供者或潜在提供者在真实世界条件下进行测试，而不受Article 60(4) points (f) and (g)所规定条件的约束。

3. 当市场监督机构已由潜在提供者、提供者或任何第三方告知严重事件，或有其他理由认为第60条和第61条规定的条件未满足时，其可酌情在其领土上采取以下任一决定：

(a) 暂停或终止在真实世界条件下的测试；

(b) 要求提供者或潜在提供者以及部署者或潜在部署者修改真实世界条件下测试的任何方面。

4. 当市场监督机构已作出本条第3款所述决定，或已发出第60(4)条(b)项含义内的异议时，该决定或异议应说明其理由以及提供者或潜在提供者如何对该决定或异议提出质疑。

5. 在适用情况下，当市场监督机构已作出第3款所述决定时，其应将理由传达给已根据测试计划对该人工智能系统进行测试的其他成员国的市场监督机构。

第77条

保护基本权利的主管机构的权力

1. 负责监督或强制执行与使用附件三所述高风险人工智能系统相关的、保护基本权利(包括不受歧视的权利)的欧盟法义务遵守情况的国家公共机构或机关，在其管辖范围内为有效履行其职责而需要查阅根据本条例创建或保存的任何文件时，有权以可访问的语言和格式请求并查阅该等文件。相关公共机构或机关应将任何此类请求告知相关成员国的市场监督机构。

2. 到2024年11月2日，每个成员国应确定第1款所指的公共机构或机关，并公布其清单。成员国应将清单通知委员会和其他成员国，并保持清单更新。

3. 当第1款所述文件不足以确定是否发生了违反保护基本权利的欧盟法义务的情况时，第1款所述公共机构或机关可向市场监督机构提出附有理由的请求，要求通过技术手段组织对高风险人工智能系统的测试。市场监督机构应在提出请求后的合理时间内，在请求方公共机构或机关的密切参与下组织测试。

4. 国家公共机构或本条第1款所述团体根据本条获得的任何信息或文件应按照第78条规定的保密义务处理。

第78条

保密

1. 委员会、市场监督机构和公告机构以及参与本条例适用的任何其他自然人或法人，应根据欧盟或国家法律，尊重在履行其任务和活动时获得的信息和数据的保密性，以特别保护：

(a) the intellectual property rights and confidential business information or trade secrets of a natural or legal person, including source code, except in the cases referred to in Article 5 of Directive (EU) 2016/943 of the European Parliament and of the Council ([57]);

(b) the effective implementation of this Regulation, in particular for the purposes of inspections, investigations or audits;

(c) public and national security interests;

(d) the conduct of criminal or administrative proceedings;

(e) information classified pursuant to Union or national law.

2. The authorities involved in the application of this Regulation pursuant to paragraph 1 shall request only data that is strictly necessary for the assessment of the risk posed by AI systems and for the exercise of their powers in accordance with this Regulation and with Regulation (EU) 2019/1020. They shall put in place adequate and effective cybersecurity measures to protect the security and confidentiality of the information and data obtained, and shall delete the data collected as soon as it is no longer needed for the purpose for which it was obtained, in accordance with applicable Union or national law.

3. Without prejudice to paragraphs 1 and 2, information exchanged on a confidential basis between the national competent authorities or between national competent authorities and the Commission shall not be disclosed without prior consultation of the originating national competent authority and the deployer when high-risk AI systems referred to in point 1, 6 or 7 of Annex III are used by law enforcement, border control, immigration or asylum authorities and when such disclosure would jeopardise public and national security interests. This exchange of information shall not cover sensitive operational data in relation to the activities of law enforcement, border control, immigration or asylum authorities.

When the law enforcement, immigration or asylum authorities are providers of high-risk AI systems referred to in point 1, 6 or 7 of Annex III, the technical documentation referred to in Annex IV shall remain within the premises of those authorities. Those authorities shall ensure that the market surveillance authorities referred to in Article 74(8) and (9), as applicable, can, upon request, immediately access the documentation or obtain a copy thereof. Only staff of the market surveillance authority holding the appropriate level of security clearance shall be allowed to access that documentation or any copy thereof.

4. Paragraphs 1, 2 and 3 shall not affect the rights or obligations of the Commission, Member States and their relevant authorities, as well as those of notified bodies, with regard to the exchange of information and the dissemination of warnings, including in the context of cross-border cooperation, nor shall they affect the obligations of the parties concerned to provide information under criminal law of the Member States.

5. The Commission and Member States may exchange, where necessary and in accordance with relevant provisions of international and trade agreements, confidential information with regulatory authorities of third countries with which they have concluded bilateral or multilateral confidentiality arrangements guaranteeing an adequate level of confidentiality.

Article 79

Procedure at national level for dealing with AI systems presenting a risk

1. AI systems presenting a risk shall be understood as a 'product presenting a risk' as defined in Article 3, point 19 of Regulation (EU) 2019/1020, in so far as they present risks to the health or safety, or to fundamental rights, of persons.

2. Where the market surveillance authority of a Member State has sufficient reason to consider an AI system to present a risk as referred to in paragraph 1 of this Article, it shall carry out an evaluation of the AI system concerned in respect of its compliance with all the requirements and obligations laid down in this Regulation. Particular attention shall be given to AI systems presenting a risk to vulnerable groups. Where risks to fundamental rights are identified, the market surveillance authority shall also inform and fully cooperate with the relevant national public authorities or bodies referred to in Article 77(1). The relevant operators shall cooperate as necessary with the market surveillance authority and with the other national public authorities or bodies referred to in Article 77(1).

([57]) Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (OJ L 157, 15.6.2016, p. 1).

(a) 自然人或法人的知识产权和保密商业信息或商业秘密，包括源代码，但欧洲议会和理事会(EU) 2016/943号指令(57)第5条所述情况除外；

(b) 本条例的有效实施，特别是为了检查、调查或审计的目的；

(c) 公共利益和国家安全利益；

(d) 进行刑事或行政程序；

(e) 根据Union或国家法律分类的信息。

2. 根据第1款参与本条例适用的各机构，仅应请求为评估人工智能系统所构成的风险以及为根据本条例和Regulation (EU) 2019/1020行使其权力所严格必需的数据。它们应实施充分且有效的网络安全措施，以保护所获得信息和数据的安全与机密性，并应根据适用的欧盟法或国家法律，在所收集数据不再为获取该数据之目的所需时尽快删除该数据。

3. 在不影响第1款和第2款的情况下，国家主管机关之间或国家主管机关与委员会之间以保密方式交换的信息，在执法、边境管制、移民或庇护当局使用附件三point 1、6或7所述高风险人工智能系统，且此类披露将危及公共和国家利益安全时，未经事先与信息来源国家主管机关和部署者协商，不得披露。此类信息交换不应涵盖与执法、边境管制、移民或庇护当局活动相关的敏感业务数据。

当执法、移民或庇护机构是附件三第1、6或7点所述高风险人工智能系统的提供者时，附件四所述技术文档应保留在这些机构的场所内。这些机构应确保第74(8)和(9)条所述市场监督机构(视情况而定)能够应请求立即访问该文档或获取其副本。仅持有适当安全许可级别的市场监督机构工作人员才允许访问该文档或其任何副本。

4. 第1、2和3款不影响委员会、成员国及其相关主管机关以及公告机构在信息交换和发布警告方面的权利或义务，包括在跨境合作背景下的权利或义务，也不影响有关各方根据成员国刑法提供信息的义务。

5. 委员会和成员国可在必要时并根据国际协定和贸易协定的相关规定，与已与其缔结双边或多边保密安排、保证适当保密水平的第三国监管机构交换保密信息。

第79条

处理构成风险的人工智能系统的国家层面程序

1.构成风险的人工智能系统应理解为(EU) 2019/1020号条例第3条第19点所定义的"构成风险的产品"，只要其对人员的健康或安全或基本权利构成风险。

2. 当成员国的市场监督机构有充分理由认为人工智能系统存在本条第1款所述风险时，该机构应就该人工智能系统对本条例规定的所有要求和义务的遵守情况进行评估。应特别关注对弱势群体构成风险的人工智能系统。如发现基本权利风险，市场监督机构还应通知第77(1)条所述的相关国家公共当局或机构并与其充分合作。相关运营者应视需要与市场监督机构及第77(1)条所述的其他国家公共当局或机构合作。

(57) 欧洲议会和理事会2016年6月8日关于保护未披露的专有技术和商业信息(商业秘密)免遭非法获取、使用和披露的(EU) 2016/943号指令(OJ L 157, 15.6.2016， 第1页)。

Where, in the course of that evaluation, the market surveillance authority or, where applicable the market surveillance authority in cooperation with the national public authority referred to in Article 77(1), finds that the AI system does not comply with the requirements and obligations laid down in this Regulation, it shall without undue delay require the relevant operator to take all appropriate corrective actions to bring the AI system into compliance, to withdraw the AI system from the market, or to recall it within a period the market surveillance authority may prescribe, and in any event within the shorter of 15 working days, or as provided for in the relevant Union harmonisation legislation.

The market surveillance authority shall inform the relevant notified body accordingly. Article 18 of Regulation (EU) 2019/1020 shall apply to the measures referred to in the second subparagraph of this paragraph.

3. Where the market surveillance authority considers that the non-compliance is not restricted to its national territory, it shall inform the Commission and the other Member States without undue delay of the results of the evaluation and of the actions which it has required the operator to take.

4. The operator shall ensure that all appropriate corrective action is taken in respect of all the AI systems concerned that it has made available on the Union market.

5. Where the operator of an AI system does not take adequate corrective action within the period referred to in paragraph 2, the market surveillance authority shall take all appropriate provisional measures to prohibit or restrict the AI system's being made available on its national market or put into service, to withdraw the product or the standalone AI system from that market or to recall it. That authority shall without undue delay notify the Commission and the other Member States of those measures.

6. The notification referred to in paragraph 5 shall include all available details, in particular the information necessary for the identification of the non-compliant AI system, the origin of the AI system and the supply chain, the nature of the non-compliance alleged and the risk involved, the nature and duration of the national measures taken and the arguments put forward by the relevant operator. In particular, the market surveillance authorities shall indicate whether the non-compliance is due to one or more of the following:

(a) non-compliance with the prohibition of the AI practices referred to in Article 5;

(b) a failure of a high-risk AI system to meet requirements set out in Chapter III, Section 2;

(c) shortcomings in the harmonised standards or common specifications referred to in Articles 40 and 41 conferring a presumption of conformity;

(d) non-compliance with Article 50.

7. The market surveillance authorities other than the market surveillance authority of the Member State initiating the procedure shall, without undue delay, inform the Commission and the other Member States of any measures adopted and of any additional information at their disposal relating to the non-compliance of the AI system concerned, and, in the event of disagreement with the notified national measure, of their objections.

8. Where, within three months of receipt of the notification referred to in paragraph 5 of this Article, no objection has been raised by either a market surveillance authority of a Member State or by the Commission in respect of a provisional measure taken by a market surveillance authority of another Member State, that measure shall be deemed justified. This shall be without prejudice to the procedural rights of the concerned operator in accordance with Article 18 of Regulation (EU) 2019/1020. The three-month period referred to in this paragraph shall be reduced to 30 days in the event of non-compliance with the prohibition of the AI practices referred to in Article 5 of this Regulation.

9. The market surveillance authorities shall ensure that appropriate restrictive measures are taken in respect of the product or the AI system concerned, such as withdrawal of the product or the AI system from their market, without undue delay.

Article 80

Procedure for dealing with AI systems classified by the provider as non-high-risk in application of Annex III

1. Where a market surveillance authority has sufficient reason to consider that an AI system classified by the provider as non-high-risk pursuant to Article 6(3) is indeed high-risk, the market surveillance authority shall carry out an evaluation of the AI system concerned in respect of its classification as a high-risk AI system based on the conditions set out in Article 6(3) and the Commission guidelines.

如果在评估过程中，市场监督机构，或在适用情况下市场监督机构与第77(1)条所述的国家公共机构合作，发现该人工智能系统不符合本条例规定的要求和义务，则应当在不无故拖延的情况下，要求相关运营者在市场监督机构规定的期限内，且在任何情况下在15个工作日内(以较短者为准)，或相关欧盟协调立法规定的期限内，采取一切适当的纠正措施使该人工智能系统合规、将该人工智能系统撤出市场或召回该人工智能系统。

市场监督机构应相应通知相关公告机构。Regulation(EU) 2019/1020第18条应适用于本款第二分段所述措施。

3. 市场监督机构认为不合规情况不限于其本国领土的，应毫不迟延地将评估结果及其要求运营者采取的行动通知委员会和其他成员国。

4. 运营者应确保对其在欧盟市场上提供的所有相关人工智能系统采取一切适当的纠正措施。

5. 如人工智能系统的运营者未在第2款所述期限内采取适当的纠正措施，市场监督机构应采取一切适当的临时措施，禁止或限制该人工智能系统在其本国市场上提供或投入使用，将该产品或独立人工智能系统从该市场撤出或召回。该机构应毫不迟延地将这些措施通知委员会和其他成员国。

6. 第5款所述通知应包含所有可获得的详细信息，特别是识别不合规人工智能系统所必需的信息、人工智能系统的来源和供应链、所指称不合规的性质和所涉风险、所采取国家措施的性质和期限以及相关运营者提出的论据。市场监督机构尤其应说明不合规是否由下列一项或多项原因所致：

(a) 不遵守第5条所述人工智能实践禁令；

(b) 高风险人工智能系统未能满足第三章第2节规定的要求；(c) 第40条和第41条所述赋予合规推定的协调标准或共同规范存在缺陷；

(d) 不遵守第50条。

7. 除发起程序的成员国的市场监督机构外，其他市场监督机构应毫不迟延地将所采取的任何措施以及其掌握的与相关人工智能系统不合规有关的任何补充信息通知委员会和其他成员国，如对已通知的国家措施有异议，还应通知其反对意见。

8. 如在本条第5款所述通知收到后三个月内，成员国市场监督机构或委员会均未对另一成员国市场监督机构采取的临时措施提出异议，该措施应被视为合理。这不应影响相关运营者依据Regulation (EU) 2019/1020第18条享有的程序性权利。如涉及不遵守本条例第5条所述人工智能实践禁令的情形，本款所述三个月期限应缩短为30天。

9. 市场监督机构应确保对相关产品或人工智能系统毫不迟延地采取适当的限制性措施，例如将产品或人工智能系统撤出其市场。

第80条

处理提供者依据附件III归类为非高风险的人工智能系统的程序

1. 市场监督机构有充分理由认为提供者依据第6(3)条归类为非高风险的人工智能系统确属高风险的，市场监督机构应基于第6(3)条规定的条件和委员会指南，就该人工智能系统作为高风险人工智能系统的分类进行评估。

2. Where, in the course of that evaluation, the market surveillance authority finds that the AI system concerned is high-risk, it shall without undue delay require the relevant provider to take all necessary actions to bring the AI system into compliance with the requirements and obligations laid down in this Regulation, as well as take appropriate corrective action within a period the market surveillance authority may prescribe.

3. Where the market surveillance authority considers that the use of the AI system concerned is not restricted to its national territory, it shall inform the Commission and the other Member States without undue delay of the results of the evaluation and of the actions which it has required the provider to take.

4. The provider shall ensure that all necessary action is taken to bring the AI system into compliance with the requirements and obligations laid down in this Regulation. Where the provider of an AI system concerned does not bring the AI system into compliance with those requirements and obligations within the period referred to in paragraph 2 of this Article, the provider shall be subject to fines in accordance with Article 99.

5. The provider shall ensure that all appropriate corrective action is taken in respect of all the AI systems concerned that it has made available on the Union market.

6. Where the provider of the AI system concerned does not take adequate corrective action within the period referred to in paragraph 2 of this Article, Article 79(5) to (9) shall apply.

7. Where, in the course of the evaluation pursuant to paragraph 1 of this Article, the market surveillance authority establishes that the AI system was misclassified by the provider as non-high-risk in order to circumvent the application of requirements in Chapter III, Section 2, the provider shall be subject to fines in accordance with Article 99.

8. In exercising their power to monitor the application of this Article, and in accordance with Article 11 of Regulation (EU) 2019/1020, market surveillance authorities may perform appropriate checks, taking into account in particular information stored in the EU database referred to in Article 71 of this Regulation.

Article 81

Union safeguard procedure

1. Where, within three months of receipt of the notification referred to in Article 79(5), or within 30 days in the case of non-compliance with the prohibition of the AI practices referred to in Article 5, objections are raised by the market surveillance authority of a Member State to a measure taken by another market surveillance authority, or where the Commission considers the measure to be contrary to Union law, the Commission shall without undue delay enter into consultation with the market surveillance authority of the relevant Member State and the operator or operators, and shall evaluate the national measure. On the basis of the results of that evaluation, the Commission shall, within six months, or within 60 days in the case of non-compliance with the prohibition of the AI practices referred to in Article 5, starting from the notification referred to in Article 79(5), decide whether the national measure is justified and shall notify its decision to the market surveillance authority of the Member State concerned. The Commission shall also inform all other market surveillance authorities of its decision.

2. Where the Commission considers the measure taken by the relevant Member State to be justified, all Member States shall ensure that they take appropriate restrictive measures in respect of the AI system concerned, such as requiring the withdrawal of the AI system from their market without undue delay, and shall inform the Commission accordingly. Where the Commission considers the national measure to be unjustified, the Member State concerned shall withdraw the measure and shall inform the Commission accordingly.

3. Where the national measure is considered justified and the non-compliance of the AI system is attributed to shortcomings in the harmonised standards or common specifications referred to in Articles 40 and 41 of this Regulation, the Commission shall apply the procedure provided for in Article 11 of Regulation (EU) No 1025/2012.

Article 82

Compliant AI systems which present a risk

1. Where, having performed an evaluation under Article 79, after consulting the relevant national public authority referred to in Article 77(1), the market surveillance authority of a Member State finds that although a high-risk AI system complies with this Regulation, it nevertheless presents a risk to the health or safety of persons, to fundamental rights, or to other aspects of public interest protection, it shall require the relevant operator to take all appropriate measures to ensure that the AI system concerned, when placed on the market or put into service, no longer presents that risk without undue delay, within a period it may prescribe.

2. 在该评估过程中，市场监督机构认定相关人工智能系统属于高风险的，应毫不迟延地要求相关提供者采取一切必要行动使该人工智能系统符合本条例规定的要求和义务，并在市场监督机构规定的期限内采取适当的纠正措施。

3. 市场监督机构认为相关人工智能系统的使用不限于其本国领土的，应毫不迟延地将评估结果及其要求提供者采取的行动通知委员会和其他成员国。

4. 提供者应确保采取一切必要行动使人工智能系统符合本条例规定的要求和义务。相关人工智能系统的提供者未在本条第2款所述期限内使该人工智能系统符合上述要求和义务的，应依照第99条受到罚款。

5. 提供者应确保对其在欧盟市场上提供的所有相关人工智能系统采取一切适当的纠正措施。

6. 相关人工智能系统的提供者未在本条第2款所述期限内采取适当纠正措施的，适用第79(5)至(9)条。

7. 在依据本条第1款进行的评估过程中，市场监督机构认定提供者为规避第三章第2节要求的适用而将该人工智能系统错误归类为非高风险的，该提供者应依照第99条受到罚款。

8. 市场监督机构在行使监督本条适用情况的权力时，可依照(EU) 2019/1020号条例第11条进行适当检查，尤其应考虑本条例第71条所述欧盟数据库中存储的信息。

第81条

联盟保障程序

1. 如在收到第79(5)条所述通知后三个月内，或在不遵守第5条所述人工智能实践禁令的情形下30天内，某成员国市场监督机构对另一市场监督机构采取的措施提出异议，或委员会认为该措施违反欧盟法律，委员会应毫不迟延地与相关成员国的市场监督机构及运营者进行磋商，并评估该国家措施。基于评估结果，委员会应自第79(5)条所述通知起六个月内，或在不遵守第5条所述人工智能实践禁令的情形下60天内，决定该国家措施是否合理，并将其决定通知相关成员国的市场监督机构。委员会还应将其决定告知所有其他市场监督机构。

2. 委员会认为相关成员国采取的措施有正当理由的，所有成员国应确保对相关人工智能系统采取适当的限制性措施，例如要求毫不迟延地将其撤出其市场，并应相应通知委员会。委员会认为国家措施无正当理由的，相关成员国应撤销该措施并相应通知委员会。

3. 国家措施被认为合理的，且人工智能系统的不合规被归因于本条例第40条和第41条所述协调标准或共同规范的缺陷的，委员会应适用(EU) No 1025/2012号条例第11条规定的程序。

第82条

存在风险的合规人工智能系统

1. 成员国市场监督机构在根据第79条进行评估后，经咨询第77(1)条所述相关国家公共机构，认定某项高风险人工智能系统虽符合本条例，但仍对人身健康或安全、基本权利或公共利益保护的其他方面构成风险的，应要求相关运营者采取一切适当措施，确保相关人工智能系统在投放市场或投入使用后毫不迟延地不再构成该风险，期限可由其规定。

2. The provider or other relevant operator shall ensure that corrective action is taken in respect of all the AI systems concerned that it has made available on the Union market within the timeline prescribed by the market surveillance authority of the Member State referred to in paragraph 1.

3. The Member States shall immediately inform the Commission and the other Member States of a finding under paragraph 1. That information shall include all available details, in particular the data necessary for the identification of the AI system concerned, the origin and the supply chain of the AI system, the nature of the risk involved and the nature and duration of the national measures taken.

4. The Commission shall without undue delay enter into consultation with the Member States concerned and the relevant operators, and shall evaluate the national measures taken. On the basis of the results of that evaluation, the Commission shall decide whether the measure is justified and, where necessary, propose other appropriate measures.

5. The Commission shall immediately communicate its decision to the Member States concerned and to the relevant operators. It shall also inform the other Member States.

Article 83

Formal non-compliance

1. Where the market surveillance authority of a Member State makes one of the following findings, it shall require the relevant provider to put an end to the non-compliance concerned, within a period it may prescribe:

(a) the CE marking has been affixed in violation of Article 48;

(b) the CE marking has not been affixed;

(c) the EU declaration of conformity referred to in Article 47 has not been drawn up;

(d) the EU declaration of conformity referred to in Article 47 has not been drawn up correctly;

(e) the registration in the EU database referred to in Article 71 has not been carried out;

(f) where applicable, no authorised representative has been appointed;

(g) technical documentation is not available.

2. Where the non-compliance referred to in paragraph 1 persists, the market surveillance authority of the Member State concerned shall take appropriate and proportionate measures to restrict or prohibit the high-risk AI system being made available on the market or to ensure that it is recalled or withdrawn from the market without delay.

Article 84

Union AI testing support structures

1. The Commission shall designate one or more Union AI testing support structures to perform the tasks listed under Article 21(6) of Regulation (EU) 2019/1020 in the area of AI.

2. Without prejudice to the tasks referred to in paragraph 1, Union AI testing support structures shall also provide independent technical or scientific advice at the request of the Board, the Commission, or of market surveillance authorities.

2. 提供者或其他相关运营者应确保在第1款所述成员国的市场监督机构规定的时限内，对其在欧盟市场上提供的所有相关人工智能系统采取纠正措施。

3. 成员国应立即将第1款下的认定结果通知委员会和其他成员国。该信息应包括所有可获得的细节，特别是识别相关人工智能系统所需的数据、该人工智能系统的来源和供应链、所涉风险的性质以及所采取国家措施的性质和期限。

4. 委员会应毫不迟延地与相关成员国和相关运营者进行磋商，并评估所采取的国家措施。委员会应根据该评估结果决定该措施是否合理，并在必要时提出其他适当措施。

5. 委员会应立即将其决定告知相关成员国和相关运营者。委员会还应通知其他成员国。

第83条

正式不合规

1. 成员国市场监督机构作出下列任一认定时，应要求相关提供者在其可规定的期限内终止有关不合规行为：

(a) CE 标志的加贴违反 Article 48;

(b) 未加贴CE标志；

(c) 第47条所述的欧盟符合性声明尚未起草；

(d) 第47条所述的欧盟符合性声明未被正确拟定；

(e) 第71条所述的在欧盟数据库中的登记尚未完成；

(f) 在适用的情况下，未指定授权代表；

(g) 技术文档不可用。

2. 第1款所述的不合规行为持续存在的，有关成员国的市场监督机构应采取适当且相称的措施，限制或禁止该高风险人工智能系统在市场上提供，或确保其立即被召回或撤出市场。

第84条

欧盟人工智能测试支持机构

1. 委员会应指定一个或多个联盟人工智能测试支持机构，在人工智能领域执行(EU) 2019/1020号条例第21(6)条所列任务。

2. 在不影响第1款所述任务的情况下，联盟人工智能测试支持机构还应应委员会、人工智能办公室或市场监督机构的请求，提供独立的技术或科学建议。

SECTION 4

Remedies

Article 85

Right to lodge a complaint with a market surveillance authority

Without prejudice to other administrative or judicial remedies, any natural or legal person having grounds to consider that there has been an infringement of the provisions of this Regulation may submit complaints to the relevant market surveillance authority.

In accordance with Regulation (EU) 2019/1020, such complaints shall be taken into account for the purpose of conducting market surveillance activities, and shall be handled in line with the dedicated procedures established therefor by the market surveillance authorities.

Article 86

Right to explanation of individual decision-making

1. Any affected person subject to a decision which is taken by the deployer on the basis of the output from a high-risk AI system listed in Annex III, with the exception of systems listed under point 2 thereof, and which produces legal effects or similarly significantly affects that person in a way that they consider to have an adverse impact on their health, safety or fundamental rights shall have the right to obtain from the deployer clear and meaningful explanations of the role of the AI system in the decision-making procedure and the main elements of the decision taken.

2. Paragraph 1 shall not apply to the use of AI systems for which exceptions from, or restrictions to, the obligation under that paragraph follow from Union or national law in compliance with Union law.

3. This Article shall apply only to the extent that the right referred to in paragraph 1 is not otherwise provided for under Union law.

Article 87

Reporting of infringements and protection of reporting persons

Directive (EU) 2019/1937 shall apply to the reporting of infringements of this Regulation and the protection of persons reporting such infringements.

SECTION 5

Supervision, investigation, enforcement and monitoring in respect of providers of general-purpose AI models

Article 88

Enforcement of the obligations of providers of general-purpose AI models

1. The Commission shall have exclusive powers to supervise and enforce Chapter V, taking into account the procedural guarantees under Article 94. The Commission shall entrust the implementation of these tasks to the AI Office, without prejudice to the powers of organisation of the Commission and the division of competences between Member States and the Union based on the Treaties.

2. Without prejudice to Article 75(3), market surveillance authorities may request the Commission to exercise the powers laid down in this Section, where that is necessary and proportionate to assist with the fulfilment of their tasks under this Regulation.

第4节

救济措施

第85条

向市场监督机构提出申诉的权利

在不影响其他行政或司法救济的情况下，任何有理由认为本条例的规定遭到违反的自然人或法人均可向相关市场监督机构提出投诉。

根据(EU) 2019/1020号条例，此类投诉应在开展市场监督活动时予以考虑，并应按照市场监督机构为此制定的专门程序进行处理。

第86条

对个人决策的解释权

1. 任何受部署者基于附件三所列高风险人工智能系统(该系统第2点所列系统除外)的输出所作决定影响的人，若该决定产生法律效力或类似地对其产生重大影响，且其认为该决定对其健康、安全或基本权利造成不利影响，则有权从部署者处获得关于人工智能系统在决策程序中所起作用的清晰且有意义的解释以及所作决定的主要要素。

2. 第1款不适用于以下人工智能系统的使用：根据符合联盟法律的联盟法或国内法，对该款所规定义务存在例外或限制的。

3. 本条仅在联盟法律未另行规定第1款所述权利的情况下适用。

第87条

违法行为的举报与举报人保护

(EU) 2019/1937号指令应适用于对本条例违规行为的举报以及对举报此类违规行为的人的保护。

第5节

对通用人工智能模型提供者的监督、调查、执行和监测

第88条

通用人工智能模型提供者义务的执行

1. 委员会应拥有监督和执行第五章的专属权力，同时考虑第94条规定的程序保障。委员会应将上述任务的实施委托给人工智能办公室，但不影响委员会的组织权力以及基于条约的成员国与联盟之间的权限划分。

2. 在不影响第75(3)条的情况下，市场监督机构可请求委员会行使本节规定的权力，前提是该请求对于协助其履行本条例下的任务是必要且相称的。

Article 89

Monitoring actions

1. For the purpose of carrying out the tasks assigned to it under this Section, the AI Office may take the necessary actions to monitor the effective implementation and compliance with this Regulation by providers of general-purpose AI models, including their adherence to approved codes of practice.

2. Downstream providers shall have the right to lodge a complaint alleging an infringement of this Regulation. A complaint shall be duly reasoned and indicate at least:

(a) the point of contact of the provider of the general-purpose AI model concerned;

(b) a description of the relevant facts, the provisions of this Regulation concerned, and the reason why the downstream provider considers that the provider of the general-purpose AI model concerned infringed this Regulation;

(c) any other information that the downstream provider that sent the request considers relevant, including, where appropriate, information gathered on its own initiative.

Article 90

Alerts of systemic risks by the scientific panel

1. The scientific panel may provide a qualified alert to the AI Office where it has reason to suspect that:

(a) a general-purpose AI model poses concrete identifiable risk at Union level; or

(b) a general-purpose AI model meets the conditions referred to in Article 51.

2. Upon such qualified alert, the Commission, through the AI Office and after having informed the Board, may exercise the powers laid down in this Section for the purpose of assessing the matter. The AI Office shall inform the Board of any measure according to Articles 91 to 94.

3. A qualified alert shall be duly reasoned and indicate at least:

(a) the point of contact of the provider of the general-purpose AI model with systemic risk concerned;

(b) a description of the relevant facts and the reasons for the alert by the scientific panel;

(c) any other information that the scientific panel considers to be relevant, including, where appropriate, information gathered on its own initiative.

Article 91

Power to request documentation and information

1. The Commission may request the provider of the general-purpose AI model concerned to provide the documentation drawn up by the provider in accordance with Articles 53 and 55, or any additional information that is necessary for the purpose of assessing compliance of the provider with this Regulation.

2. Before sending the request for information, the AI Office may initiate a structured dialogue with the provider of the general-purpose AI model.

3. Upon a duly substantiated request from the scientific panel, the Commission may issue a request for information to a provider of a general-purpose AI model, where the access to information is necessary and proportionate for the fulfilment of the tasks of the scientific panel under Article 68(2).

第89条

监测行动

1. 为执行本节赋予人工智能办公室的任务，人工智能办公室可采取必要行动，监测通用人工智能模型提供者对本条例的有效实施和遵守情况，包括其对经批准的行为准则的遵守情况。

2. 下游提供者有权提出投诉，指控违反本条例。投诉应说明充分理由，并至少指明：

(a) 所涉通用人工智能模型提供者的联络点；

(b) 相关事实的描述、本条例的相关规定，以及下游提供者认为有关通用人工智能模型提供者违反本条例的理由；

(c) 提出请求的下游提供者认为相关的任何其他信息，包括在适当情况下其自行收集的信息。

第90条

科学小组关于系统性风险的警报

1. 科学小组在有理由怀疑下列情形时，可向人工智能办公室提供限定性警报：

(a) 通用人工智能模型在联盟层面构成具体可识别的风险；或

(b) 通用人工智能模型满足第51条所述条件。

2. 收到该限定性警报后，委员会可通过人工智能办公室并在通知委员会后，为评估该事项行使本节规定的权力。人工智能办公室应根据第91条至第94条向委员会通报任何措施。

3. 合格警报应经过充分论证，并至少指明：

(a) 有关具有系统性风险的通用人工智能模型提供者的联络点；

(b) 科学小组对相关事实的描述及发出警报的理由；

(c) 科学小组认为相关的任何其他信息，包括在适当情况下其自行收集的信息。

第91条

要求提供文件与信息的权力

1. 委员会可要求有关通用人工智能模型提供者提供其根据第53条和第55条拟定的文件，或为评估该提供者遵守本条例情况所必需的任何补充信息。

2. 在发出信息请求之前，人工智能办公室可启动与通用人工智能模型提供者的结构化对话。

3. 在科学小组提出有充分理由的请求时，委员会可向通用人工智能模型提供者发出信息请求，前提是获取信息对于科学小组履行第68(2)条下的任务是必要且相称的。

4. The request for information shall state the legal basis and the purpose of the request, specify what information is required, set a period within which the information is to be provided, and indicate the fines provided for in Article 101 for supplying incorrect, incomplete or misleading information.

5. The provider of the general-purpose AI model concerned, or its representative shall supply the information requested. In the case of legal persons, companies or firms, or where the provider has no legal personality, the persons authorised to represent them by law or by their statutes, shall supply the information requested on behalf of the provider of the general-purpose AI model concerned. Lawyers duly authorised to act may supply information on behalf of their clients. The clients shall nevertheless remain fully responsible if the information supplied is incomplete, incorrect or misleading.

Article 92

Power to conduct evaluations

1. The AI Office, after consulting the Board, may conduct evaluations of the general-purpose AI model concerned:

(a) to assess compliance of the provider with obligations under this Regulation, where the information gathered pursuant to Article 91 is insufficient; or

(b) to investigate systemic risks at Union level of general-purpose AI models with systemic risk, in particular following a qualified alert from the scientific panel in accordance with Article 90(1), point (a).

2. The Commission may decide to appoint independent experts to carry out evaluations on its behalf, including from the scientific panel established pursuant to Article 68. Independent experts appointed for this task shall meet the criteria outlined in Article 68(2).

3. For the purposes of paragraph 1, the Commission may request access to the general-purpose AI model concerned through APIs or further appropriate technical means and tools, including source code.

4. The request for access shall state the legal basis, the purpose and reasons of the request and set the period within which the access is to be provided, and the fines provided for in Article 101 for failure to provide access.

5. The providers of the general-purpose AI model concerned or its representative shall supply the information requested. In the case of legal persons, companies or firms, or where the provider has no legal personality, the persons authorised to represent them by law or by their statutes, shall provide the access requested on behalf of the provider of the general-purpose AI model concerned.

6. The Commission shall adopt implementing acts setting out the detailed arrangements and the conditions for the evaluations, including the detailed arrangements for involving independent experts, and the procedure for the selection thereof. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 98(2).

7. Prior to requesting access to the general-purpose AI model concerned, the AI Office may initiate a structured dialogue with the provider of the general-purpose AI model to gather more information on the internal testing of the model, internal safeguards for preventing systemic risks, and other internal procedures and measures the provider has taken to mitigate such risks.

Article 93

Power to request measures

1. Where necessary and appropriate, the Commission may request providers to:

(a) take appropriate measures to comply with the obligations set out in Articles 53 and 54;

4. 信息请求应说明请求的法律依据和目的，明确所需信息，设定提供信息的期限，并指明第101条对提供不正确、不完整或误导性信息所规定的罚款。

5. 相关通用人工智能模型的提供者或其代表应提供所要求的信息。对于法人、公司或商号，或提供者不具有法律人格的情形，由法律或章程授权代表他们的人员代表相关通用人工智能模型的提供者提供所要求的信息。经正式授权行事的律师可代表其客户提供信息。但若所提供的信息不完整、不正确或具有误导性，客户仍应承担全部责任。

第92条

进行评价的权力

1. 人工智能办公室在咨询委员会后，可对有关通用人工智能模型进行评估：

(a) 在根据第91条收集的信息不足时，评估提供者遵守本条例义务的情况；或

(b) 调查具有系统性风险的通用人工智能模型在联盟层面的系统性风险，特别是在科学小组根据第90(1)条(a)点发出限定性警报之后。

2. 委员会可决定任命独立专家代表其进行评估，包括从根据第68条设立的科学小组中任命。为此任务任命的独立专家应符合第68(2)条所列标准。

3. 为第1款之目的，委员会可请求通过API或其他适当的技术手段和工具(包括源代码)访问有关通用人工智能模型。

4. 访问请求应说明法律依据、目的和理由，设定提供访问的期限，并指明第101条对未能提供访问所规定的罚款。

5. 有关通用人工智能模型的提供者或其代表应提供所要求的信息。对于法人、公司或商行，或者提供者不具有法律人格的情形，由法律或章程授权代表其的人员代表有关通用人工智能模型的提供者提供所要求的访问权限。

6. 委员会应通过实施法案，规定评估的详细安排和条件，包括独立专家参与的详细安排及其遴选程序。该等实施法案应按照第98(2)条所指的审查程序通过。

7. 在请求访问相关通用人工智能模型之前，人工智能办公室可启动与该通用人工智能模型提供者的结构化对话，以收集更多关于该模型内部测试、防止系统性风险的内部保障措施以及提供者为减轻此类风险而采取的其他内部程序和措施的信息。

第93条

要求采取措施的权力

1. 在必要且适当时，委员会可要求提供者：

(a) 采取适当措施遵守第53条和第54条规定的义务；

(b) implement mitigation measures, where the evaluation carried out in accordance with Article 92 has given rise to serious and substantiated concern of a systemic risk at Union level;

(c) restrict the making available on the market, withdraw or recall the model.

2. Before a measure is requested, the AI Office may initiate a structured dialogue with the provider of the general-purpose AI model.

3. If, during the structured dialogue referred to in paragraph 2, the provider of the general-purpose AI model with systemic risk offers commitments to implement mitigation measures to address a systemic risk at Union level, the Commission may, by decision, make those commitments binding and declare that there are no further grounds for action.

Article 94

Procedural rights of economic operators of the general-purpose AI model

Article 18 of Regulation (EU) 2019/1020 shall apply *mutatis mutandis* to the providers of the general-purpose AI model, without prejudice to more specific procedural rights provided for in this Regulation.

CHAPTER X

CODES OF CONDUCT AND GUIDELINES

Article 95

Codes of conduct for voluntary application of specific requirements

1. The AI Office and the Member States shall encourage and facilitate the drawing up of codes of conduct, including related governance mechanisms, intended to foster the voluntary application to AI systems, other than high-risk AI systems, of some or all of the requirements set out in Chapter III, Section 2 taking into account the available technical solutions and industry best practices allowing for the application of such requirements.

2. The AI Office and the Member States shall facilitate the drawing up of codes of conduct concerning the voluntary application, including by deployers, of specific requirements to all AI systems, on the basis of clear objectives and key performance indicators to measure the achievement of those objectives, including elements such as, but not limited to:

(a) applicable elements provided for in Union ethical guidelines for trustworthy AI;

(b) assessing and minimising the impact of AI systems on environmental sustainability, including as regards energy-efficient programming and techniques for the efficient design, training and use of AI;

(c) promoting AI literacy, in particular that of persons dealing with the development, operation and use of AI;

(d) facilitating an inclusive and diverse design of AI systems, including through the establishment of inclusive and diverse development teams and the promotion of stakeholders' participation in that process;

(e) assessing and preventing the negative impact of AI systems on vulnerable persons or groups of vulnerable persons, including as regards accessibility for persons with a disability, as well as on gender equality.

3. Codes of conduct may be drawn up by individual providers or deployers of AI systems or by organisations representing them or by both, including with the involvement of any interested stakeholders and their representative organisations, including civil society organisations and academia. Codes of conduct may cover one or more AI systems taking into account the similarity of the intended purpose of the relevant systems.

4. The AI Office and the Member States shall take into account the specific interests and needs of SMEs, including start-ups, when encouraging and facilitating the drawing up of codes of conduct.

(b) 在根据第92条进行的评估已引起对欧盟层面系统性风险的严重且有充分依据的关切时，实施缓解措施；

(c) 限制该模型投放市场、撤回或召回该模型。

2. 在请求采取某项措施之前，人工智能办公室可启动与通用人工智能模型提供者的结构化对话。

3. 如果在第2段所述的结构化对话期间，具有系统性风险的通用人工智能模型的提供者承诺实施缓解措施以应对欧盟层面的系统性风险，委员会可通过决定使这些承诺具有约束力，并宣布不再有采取进一步行动的理由。

第94条

通用人工智能模型经济运营者的程序性权利

条例(EU) 2019/1020第18条应比照适用于通用人工智能模型的提供者，不影响本条例规定的更具体的程序性权利。

第十章

行为准则与指南

第95条

自愿适用特定要求的行为准则

1. 人工智能办公室和成员国应鼓励和促进制定行为准则，包括相关治理机制，旨在促进对高风险人工智能系统以外的人工智能系统自愿适用第三章第2节所列部分或全部要求，同时考虑到允许适用此类要求的现有技术解决方案和行业最佳实践。

2. 人工智能办公室和成员国应促进制定行为准则，涉及包括由部署者自愿对所有人工智能系统适用特定要求，其基础是明确的目标和衡量这些目标实现情况的关键绩效指标，包括但不限于以下要素：

(a) 联盟可信人工智能伦理准则中规定的适用要素；

(b) 评估和尽量减少人工智能系统对环境可持续性的影响，包括在节能编程以及人工智能的高效设计、训练和使用技术方面；

(c) 促进人工智能素养，特别是从事人工智能开发、运行和使用的人员的人工智能素养；

(d) 促进人工智能系统的包容性和多样化设计，包括通过建立包容性和多样化的开发团队以及促进利益相关者参与该过程；

(e) 评估和防止人工智能系统对弱势人员或弱势群体以及性别平等的负面影响，包括在残疾人无障碍方面。

3. 行为准则可由人工智能系统的个别提供者或部署者制定，或由代表他们的组织制定，或由两者共同制定，包括任何有兴趣的利益相关者及其代表组织，包括民间社会组织和学术界的参与。行为准则可涵盖一个或多个人工智能系统，同时考虑到相关系统预期用途的相似性。

4. 人工智能办公室和成员国在鼓励和促进制定行为准则时，应考虑到中小企业(包括初创企业)的具体利益和需求。

Article 96

Guidelines from the Commission on the implementation of this Regulation

1. The Commission shall develop guidelines on the practical implementation of this Regulation, and in particular on:

(a) the application of the requirements and obligations referred to in Articles 8 to 15 and in Article 25;

(b) the prohibited practices referred to in Article 5;

(c) the practical implementation of the provisions related to substantial modification;

(d) the practical implementation of transparency obligations laid down in Article 50;

(e) detailed information on the relationship of this Regulation with the Union harmonisation legislation listed in Annex I, as well as with other relevant Union law, including as regards consistency in their enforcement;

(f) the application of the definition of an AI system as set out in Article 3, point (1).

When issuing such guidelines, the Commission shall pay particular attention to the needs of SMEs including start-ups, of local public authorities and of the sectors most likely to be affected by this Regulation.

The guidelines referred to in the first subparagraph of this paragraph shall take due account of the generally acknowledged state of the art on AI, as well as of relevant harmonised standards and common specifications that are referred to in Articles 40 and 41, or of those harmonised standards or technical specifications that are set out pursuant to Union harmonisation law.

2. At the request of the Member States or the AI Office, or on its own initiative, the Commission shall update guidelines previously adopted when deemed necessary.

CHAPTER XI

DELEGATION OF POWER AND COMMITTEE PROCEDURE

Article 97

Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The power to adopt delegated acts referred to in Article 6(6) and (7), Article 7(1) and (3), Article 11(3), Article 43(5) and (6), Article 47(5), Article 51(3), Article 52(4) and Article 53(5) and (6) shall be conferred on the Commission for a period of five years from 1 August 2024. The Commission shall draw up a report in respect of the delegation of power not later than nine months before the end of the five-year period. The delegation of power shall be tacitly extended for periods of an identical duration, unless the European Parliament or the Council opposes such extension not later than three months before the end of each period.

3. The delegation of power referred to in Article 6(6) and (7), Article 7(1) and (3), Article 11(3), Article 43(5) and (6), Article 47(5), Article 51(3), Article 52(4) and Article 53(5) and (6) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following that of its publication in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.

第96条

委员会关于本条例实施的指南

1. 委员会应制定关于本条例实际实施的指南，特别是关于：

(a) 第8条至第15条和第25条所述要求和义务的适用；

(b) 第5条所禁止的做法；

(c) 与实质性修改相关的条款的实际实施；

(d) 第50条规定的透明度义务的实际实施；

(e) 关于本条例与附件一所列欧盟协调立法以及其他相关欧盟法律之间关系的详细信息，包括在其执行一致性方面；

(f) 第3条第(1)点所规定的人工智能系统定义的应用。

在发布此类指南时，委员会应特别关注中小企业(包括初创企业)、地方公共当局以及最可能受本条例影响的部门的需求。

本款第一项所述的指南应适当考虑人工智能领域普遍公认的技术水平，以及第40条和第41条所述的相关协调标准和通用规范，或根据联盟协调法制定的协调标准或技术规范。

2. 应成员国或人工智能办公室的请求，或主动地，委员会应在认为必要时更新先前通过的指南。

第十一章

权力下放与委员会程序

第97条

授权的行使

1. 授予委员会通过授权法案的权力须遵守本条规定的条件。

2. 第6条第(6)款和第(7)款、第7条第(1)款和第(3)款、第11条第(3)款、第43条第(5)款和第(6)款、第47条第(5)款、第51条第(3)款、第52条第(4)款以及第53条第(5)款和第(6)款所述通过授权法案的权力，应自2024年8月1日起授予委员会，为期五年。委员会应在该五年期结束前不迟于九个月就权力委托起草一份报告。除非欧洲议会或理事会在每期结束前不迟于三个月反对此种延长，否则权力委托应默示延长相同期限。

3. 第6条第(6)款和第(7)款、第7条第(1)款和第(3)款、第11条第(3)款、第43条第(5)款和第(6)款、第47条第(5)款、第51条第(3)款、第52条第(4)款以及第53条第(5)款和第(6)款所述的权力委托，可由欧洲议会或理事会随时撤销。撤销决定应终止该决定中指定的权力委托。该决定应在其于欧盟官方公报上公布之日的次日起生效，或在其指定的较后日期生效。该决定不影响已生效的任何授权法案的有效性。

4. 在通过授权法案之前，委员会应根据2016年4月13日《关于改进立法的机构间协议》所规定的原则，咨询各成员国指定的专家。

5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

6. Any delegated act adopted pursuant to Article 6(6) or (7), Article 7(1) or (3), Article 11(3), Article 43(5) or (6), Article 47(5), Article 51(3), Article 52(4) or Article 53(5) or (6) shall enter into force only if no objection has been expressed by either the European Parliament or the Council within a period of three months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by three months at the initiative of the European Parliament or of the Council.

Article 98

Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

CHAPTER XII

PENALTIES

Article 99

Penalties

1. In accordance with the terms and conditions laid down in this Regulation, Member States shall lay down the rules on penalties and other enforcement measures, which may also include warnings and non-monetary measures, applicable to infringements of this Regulation by operators, and shall take all measures necessary to ensure that they are properly and effectively implemented, thereby taking into account the guidelines issued by the Commission pursuant to Article 96. The penalties provided for shall be effective, proportionate and dissuasive. They shall take into account the interests of SMEs, including start-ups, and their economic viability.

2. The Member States shall, without delay and at the latest by the date of entry into application, notify the Commission of the rules on penalties and of other enforcement measures referred to in paragraph 1, and shall notify it, without delay, of any subsequent amendment to them.

3. Non-compliance with the prohibition of the AI practices referred to in Article 5 shall be subject to administrative fines of up to EUR 35 000 000 or, if the offender is an undertaking, up to 7 % of its total worldwide annual turnover for the preceding financial year, whichever is higher.

4. Non-compliance with any of the following provisions related to operators or notified bodies, other than those laid down in Articles 5, shall be subject to administrative fines of up to EUR 15 000 000 or, if the offender is an undertaking, up to 3 % of its total worldwide annual turnover for the preceding financial year, whichever is higher:

(a) obligations of providers pursuant to Article 16;

(b) obligations of authorised representatives pursuant to Article 22;

(c) obligations of importers pursuant to Article 23;

(d) obligations of distributors pursuant to Article 24;

(e) obligations of deployers pursuant to Article 26;

(f) requirements and obligations of notified bodies pursuant to Article 31, Article 33(1), (3) and (4) or Article 34;

(g) transparency obligations for providers and deployers pursuant to Article 50.

5. 委员会在通过授权法案后，应同时通知欧洲议会和理事会。

6. 依据第6条第(6)款或第(7)款、第7条第(1)款或第(3)款、第11条第(3)款、第43条第(5)款或第(6)款、第47条第(5)款、第51条第(3)款、第52条第(4)款或第53条第(5)款或第(6)款通过的任何授权法案，只有在欧洲议会或理事会在该法案通知欧洲议会和理事会后三个月内未表示反对，或者在该期限届满前欧洲议会和理事会均已通知委员会其不会反对的情况下，方可生效。该期限应因欧洲议会或理事会的提议而延长三个月。

第98条

委员会程序

1. 委员会应由一个委员会协助。该委员会应为第182/2011号条例(欧盟)含义内的委员会。

2. 凡提及本段时，应适用第182/2011号条例(欧盟)第5条。

第十二章

处罚

第99条

处罚

1. 依照本条例规定的条款和条件，成员国应制定关于处罚和其他执法措施的规则，其中也可包括警告和非金钱措施，适用于运营者违反本条例的行为，并应采取一切必要措施确保其得到适当和有效的实施，同时考虑到委员会依据第96条发布的指南。所规定的处罚应有效、相称且具有威慑力。处罚应考虑SME(包括初创企业)的利益及其经济可行性。

2. 成员国应毫不迟延地且最迟在适用之日，向委员会通报第1段所述的处罚规则和其他执法措施，并应毫不迟延地向其通报随后的任何修订。

3. 不遵守第5条所述禁止的人工智能实践，应处以最高35 000 000欧元的行政罚款，如果违法者是企业，则处以最高为其上一财政年度全球年总营业额7%的行政罚款，以较高者为准。

4. 不遵守以下与运营者或公告机构相关的任何规定(第5条所列规定除外)，应处以最高15 000 000欧元的行政罚款，如果违法者是企业，则处以最高为其上一财政年度全球年总营业额3%的行政罚款，以较高者为准：

(a) 第16条规定的提供者义务；

(b) 第22条规定的授权代表的义务；

(c) 第23条规定的进口商义务；

(d) 分销商依据第24条承担的义务；

(e) 部署者根据第26条承担的义务；(f) 公告机构根据第31条、第33条第(1)、(3)和(4)款或第34条承担的要求和义务；(g) 提供者和部署者根据第50条承担的透明度义务。

5. The supply of incorrect, incomplete or misleading information to notified bodies or national competent authorities in reply to a request shall be subject to administrative fines of up to EUR 7 500 000 or, if the offender is an undertaking, up to 1 % of its total worldwide annual turnover for the preceding financial year, whichever is higher.

6. In the case of SMEs, including start-ups, each fine referred to in this Article shall be up to the percentages or amount referred to in paragraphs 3, 4 and 5, whichever thereof is lower.

7. When deciding whether to impose an administrative fine and when deciding on the amount of the administrative fine in each individual case, all relevant circumstances of the specific situation shall be taken into account and, as appropriate, regard shall be given to the following:

(a) the nature, gravity and duration of the infringement and of its consequences, taking into account the purpose of the AI system, as well as, where appropriate, the number of affected persons and the level of damage suffered by them;

(b) whether administrative fines have already been applied by other market surveillance authorities to the same operator for the same infringement;

(c) whether administrative fines have already been applied by other authorities to the same operator for infringements of other Union or national law, when such infringements result from the same activity or omission constituting a relevant infringement of this Regulation;

(d) the size, the annual turnover and market share of the operator committing the infringement;

(e) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement;

(f) the degree of cooperation with the national competent authorities, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(g) the degree of responsibility of the operator taking into account the technical and organisational measures implemented by it;

(h) the manner in which the infringement became known to the national competent authorities, in particular whether, and if so to what extent, the operator notified the infringement;

(i) the intentional or negligent character of the infringement;

(j) any action taken by the operator to mitigate the harm suffered by the affected persons.

8. Each Member State shall lay down rules on to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

9. Depending on the legal system of the Member States, the rules on administrative fines may be applied in such a manner that the fines are imposed by competent national courts or by other bodies, as applicable in those Member States. The application of such rules in those Member States shall have an equivalent effect.

10. The exercise of powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and national law, including effective judicial remedies and due process.

11. Member States shall, on an annual basis, report to the Commission about the administrative fines they have issued during that year, in accordance with this Article, and about any related litigation or judicial proceedings.

Article 100

Administrative fines on Union institutions, bodies, offices and agencies

1. The European Data Protection Supervisor may impose administrative fines on Union institutions, bodies, offices and agencies falling within the scope of this Regulation. When deciding whether to impose an administrative fine and when deciding on the amount of the administrative fine in each individual case, all relevant circumstances of the specific situation shall be taken into account and due regard shall be given to the following:

5. 在答复请求时向公告机构或国家主管机关提供不正确、不完整或误导性信息，应处以最高7 500 000欧元的行政罚款，如果违法者是企业，则处以最高为其上一财政年度全球年总营业额1%的行政罚款，以较高者为准。

6. 对于中小企业(包括初创企业)，本条所述的每项罚款应不超过第3、4和5段所述的百分比或金额，以其中较低者为准。

7. 在决定是否处以行政罚款以及在决定每个个案中行政罚款的金额时，应考虑具体情况的所有相关情节，并酌情考虑以下因素：

(a) 侵权及其后果的性质、严重程度和持续时间，同时考虑到人工智能系统的用途，以及酌情考虑受影响人数和他们所受损害的程度；

(b) 其他市场监督机构是否已因同一侵权行为对同一运营者处以行政罚款；

(c) 其他机关是否已因同一运营者违反其他欧盟或国家法律而对其处以行政罚款，且该等违法行为与构成本条例相关违法行为的行为或不作为相同；

(d) 实施违法行为的运营者的规模、年营业额和市场份额；

(e) 适用于案件具体情形的任何其他加重或减轻情节，例如直接或间接从违法行为中获得的财务利益或避免的损失；

(f) 与国家主管机关合作以纠正违法行为并减轻违法行为可能造成的不利影响的程度；

(g) 运营者的责任程度，同时考虑其已实施的技术和组织措施；

(h) 国家主管机关获悉违法行为的方式，特别是运营者是否通报了违法行为以及通报的程度；

(i) 侵权的故意或过失性质；

(j) 运营者为减轻受影响人员所受损害而采取的任何行动。

8. 各成员国应就可在多大程度上对设于该成员国的公共机关和机构处以行政罚款制定规则。

9. 视成员国的法律制度而定，关于行政罚款的规则可按由主管国家法院或其他机构处以罚款的方式适用，具体视各成员国的情况而定。此类规则在这些成员国的适用应具有同等效力。

10. 依本条行使权力应遵守符合欧盟法和国家法的适当程序保障，包括有效的司法救济和正当程序。

11. 成员国应每年向委员会报告其在该年度内依照本条作出的行政罚款以及任何相关诉讼或司法程序。

第100条

对欧盟机构、机关、办事处和机构的行政罚款

1. 欧洲数据保护监督员可对本条例适用范围内的欧盟机构、机关、办事处和机构处以行政罚款。在决定是否处以行政罚款以及决定每个个案中行政罚款的金额时，应考虑具体情况的所有相关情节，并适当顾及以下各项：

(a) the nature, gravity and duration of the infringement and of its consequences, taking into account the purpose of the AI system concerned, as well as, where appropriate, the number of affected persons and the level of damage suffered by them;

(b) the degree of responsibility of the Union institution, body, office or agency, taking into account technical and organisational measures implemented by them;

(c) any action taken by the Union institution, body, office or agency to mitigate the damage suffered by affected persons;

(d) the degree of cooperation with the European Data Protection Supervisor in order to remedy the infringement and mitigate the possible adverse effects of the infringement, including compliance with any of the measures previously ordered by the European Data Protection Supervisor against the Union institution, body, office or agency concerned with regard to the same subject matter;

(e) any similar previous infringements by the Union institution, body, office or agency;

(f) the manner in which the infringement became known to the European Data Protection Supervisor, in particular whether, and if so to what extent, the Union institution, body, office or agency notified the infringement;

(g) the annual budget of the Union institution, body, office or agency.

2. Non-compliance with the prohibition of the AI practices referred to in Article 5 shall be subject to administrative fines of up to EUR 1 500 000.

3. The non-compliance of the AI system with any requirements or obligations under this Regulation, other than those laid down in Article 5, shall be subject to administrative fines of up to EUR 750 000.

4. Before taking decisions pursuant to this Article, the European Data Protection Supervisor shall give the Union institution, body, office or agency which is the subject of the proceedings conducted by the European Data Protection Supervisor the opportunity of being heard on the matter regarding the possible infringement. The European Data Protection Supervisor shall base his or her decisions only on elements and circumstances on which the parties concerned have been able to comment. Complainants, if any, shall be associated closely with the proceedings.

5. The rights of defence of the parties concerned shall be fully respected in the proceedings. They shall be entitled to have access to the European Data Protection Supervisor's file, subject to the legitimate interest of individuals or undertakings in the protection of their personal data or business secrets.

6. Funds collected by imposition of fines in this Article shall contribute to the general budget of the Union. The fines shall not affect the effective operation of the Union institution, body, office or agency fined.

7. The European Data Protection Supervisor shall, on an annual basis, notify the Commission of the administrative fines it has imposed pursuant to this Article and of any litigation or judicial proceedings it has initiated.

Article 101

Fines for providers of general-purpose AI models

1. The Commission may impose on providers of general-purpose AI models fines not exceeding 3 % of their annual total worldwide turnover in the preceding financial year or EUR 15 000 000, whichever is higher., when the Commission finds that the provider intentionally or negligently:

(a) infringed the relevant provisions of this Regulation;

(b) failed to comply with a request for a document or for information pursuant to Article 91, or supplied incorrect, incomplete or misleading information;

(c) failed to comply with a measure requested under Article 93;

(a) 违法行为的性质、严重程度和持续时间及其后果，同时考虑相关人工智能系统的目的，以及酌情考虑受影响人员的数量和其所受损害的程度；

(b) 欧盟机构、机关、办事处或机构的责任程度，同时考虑其已实施的技术和组织措施；

(c) 欧盟机构、机关、办事处或机构为减轻受影响人员所受损害而采取的任何行动；

(d) 与欧洲数据保护监督员合作以纠正违法行为并减轻违法行为可能造成的不利影响的程度，包括遵守欧洲数据保护监督员此前就同一事项对相关欧盟机构、机关、办事处或机构命令采取的任何措施；

(e) 该联盟机构、机关、办事处或机构此前是否有任何类似侵权行为；

(f) 欧洲数据保护监督员获悉违法行为的方式，特别是欧盟机构、机关、办事处或机构是否通报了违法行为以及通报的程度；

(g) 欧盟机构、机关、办事处或机构的年度预算。

2. 不遵守Article 5所述禁止的人工智能实践的，应处以最高1 500 000欧元的行政罚款。

3. 人工智能系统不符合本条例规定的除Article 5所规定者以外的任何要求或义务的，应处以最高750 000欧元的行政罚款。

4. 在依据本条作出决定之前，欧洲数据保护监督员应给予作为欧洲数据保护监督员所进行程序对象的联盟机构、机关、办公室或机构就可能的侵权行为事项发表意见的机会。欧洲数据保护监督员应仅基于有关当事方能够发表意见的要素和情况作出其决定。如有投诉人，应使其密切参与程序。

5. 在程序中应充分尊重有关各方的辩护权。他们应有权查阅欧洲数据保护监督员的案卷，但须顾及个人或企业在保护其个人数据或商业秘密方面的合法利益。

6. 依本条处以罚款所收取的资金应纳入欧盟总预算。罚款不得影响被罚款的欧盟机构、机关、办事处或机构的有效运作。

7. 欧洲数据保护监督员应每年向委员会通报其依照本条处以的行政罚款以及其提起的任何诉讼或司法程序。

第101条

对通用人工智能模型提供者的罚款

1. 当委员会认定通用人工智能模型的提供者故意或过失地有下列情形时，委员会可对该提供者处以不超过其上一财政年度全球年总营业额3%或15 000 000欧元的罚款，以较高者为准：

(a) 违反了本条例的相关规定；

(b) 未遵守依Article 91提出的文件或信息请求，或提供了不正确、不完整或误导性的信息；

(c) 未遵守根据第93条要求的措施；

(d) failed to make available to the Commission access to the general-purpose AI model or general-purpose AI model with systemic risk with a view to conducting an evaluation pursuant to Article 92.

In fixing the amount of the fine or periodic penalty payment, regard shall be had to the nature, gravity and duration of the infringement, taking due account of the principles of proportionality and appropriateness. The Commission shall also into account commitments made in accordance with Article 93(3) or made in relevant codes of practice in accordance with Article 56.

2. Before adopting the decision pursuant to paragraph 1, the Commission shall communicate its preliminary findings to the provider of the general-purpose AI model and give it an opportunity to be heard.

3. Fines imposed in accordance with this Article shall be effective, proportionate and dissuasive.

4. Information on fines imposed under this Article shall also be communicated to the Board as appropriate.

5. The Court of Justice of the European Union shall have unlimited jurisdiction to review decisions of the Commission fixing a fine under this Article. It may cancel, reduce or increase the fine imposed.

6. The Commission shall adopt implementing acts containing detailed arrangements and procedural safeguards for proceedings in view of the possible adoption of decisions pursuant to paragraph 1 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 98(2).

CHAPTER XIII

FINAL PROVISIONS

Article 102

Amendment to Regulation (EC) No 300/2008

In Article 4(3) of Regulation (EC) No 300/2008, the following subparagraph is added:

'When adopting detailed measures related to technical specifications and procedures for approval and use of security equipment concerning Artificial Intelligence systems within the meaning of Regulation (EU) 2024/1689 of the European Parliament and of the Council (*), the requirements set out in Chapter III, Section 2, of that Regulation shall be taken into account.

(*) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (OJ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).'.

Article 103

Amendment to Regulation (EU) No 167/2013

In Article 17(5) of Regulation (EU) No 167/2013, the following subparagraph is added:

'When adopting delegated acts pursuant to the first subparagraph concerning artificial intelligence systems which are safety components within the meaning of Regulation (EU) 2024/1689 of the European Parliament and of the Council (*), the requirements set out in Chapter III, Section 2, of that Regulation shall be taken into account.

(*) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (OJ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).'.

(d) 未向委员会提供对通用人工智能模型或具有系统性风险的通用人工智能模型的访问，以便依Article 92进行评价。

在确定罚款或定期罚款金额时，应考虑侵权行为的性质、严重程度和持续时间，并适当考虑相称性和适当性原则。委员会还应考虑依据第93(3)条作出的承诺或依据第56条在相关行为准则中作出的承诺。

2. 在依第1款作出决定之前，委员会应将其初步调查结果告知通用人工智能模型的提供者，并给予其陈述意见的机会。

3. 依照本条处以的罚款应有效、相称且具有威慑力。

4. 关于依本条处以罚款的信息也应酌情通报委员会。

5. 欧盟法院对委员会依本条确定罚款的决定拥有无限管辖权。欧盟法院可撤销、减少或增加所处以的罚款。

6. 委员会应通过实施法案，其中包含针对可能根据本条第1款通过决定的程序的详细安排和程序保障。该等实施法案应按照第98条第2款所指的审查程序通过。

第十三章

最终条款

第102条

对第300/2008号条例(EC)的修订

在第300/2008号条例(EC)第4(3)条中，增加以下分段：

“在通过有关欧洲议会和理事会条例(EU) 2024/1689(*)所指人工智能系统安全设备的批准和使用的技术规范和程序的详细措施时，应考虑到该条例第三章第2节规定的要求。

(*) 欧洲议会和理事会2024年6月13日第(EU) 2024/1689号条例，规定统一规则并修订条例(EC) No 300/2008、(EU) No 167/2013、(EU) No 168/2013、(EU) 2018/858、(EU) 2018/1139和(EU) 2019/2144以及指令2014/90/EU、(EU) 2016/797和(EU) 2020/1828(人工智能法案)(OJ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/ 2024/1689/oj)。”。

第103条

对第167/2013号条例(EU)的修订

在第167/2013号条例(欧盟)第17(5)条中，增加以下分段：

“在根据第一小段通过有关属于欧洲议会和理事会条例(EU) 2024/1689(*)所指安全组件的人工智能系统的授权法案时，应考虑到该条例第三章第2节规定的要求。

(*) 欧洲议会和理事会2024年6月13日第(EU) 2024/1689号条例，规定统一规则并修订条例(EC) No 300/2008、(EU) No 167/2013、(EU) No 168/2013、(EU) 2018/858、(EU) 2018/1139和(EU) 2019/2144以及指令2014/90/EU、(EU) 2016/797和(EU) 2020/1828(人工智能法案)(OJ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/ 2024/1689/oj)。”。

Article 104

Amendment to Regulation (EU) No 168/2013

In Article 22(5) of Regulation (EU) No 168/2013, the following subparagraph is added:

‘When adopting delegated acts pursuant to the first subparagraph concerning Artificial Intelligence systems which are safety components within the meaning of Regulation (EU) 2024/1689 of the European Parliament and of the Council (*), the requirements set out in Chapter III, Section 2, of that Regulation shall be taken into account.

(*) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (OJ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).’.

Article 105

Amendment to Directive 2014/90/EU

In Article 8 of Directive 2014/90/EU, the following paragraph is added:

‘5. For Artificial Intelligence systems which are safety components within the meaning of Regulation (EU) 2024/1689 of the European Parliament and of the Council (*), when carrying out its activities pursuant to paragraph 1 and when adopting technical specifications and testing standards in accordance with paragraphs 2 and 3, the Commission shall take into account the requirements set out in Chapter III, Section 2, of that Regulation.

(*) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (OJ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).’.

Article 106

Amendment to Directive (EU) 2016/797

In Article 5 of Directive (EU) 2016/797, the following paragraph is added:

‘12. When adopting delegated acts pursuant to paragraph 1 and implementing acts pursuant to paragraph 11 concerning Artificial Intelligence systems which are safety components within the meaning of Regulation (EU) 2024/1689 of the European Parliament and of the Council (*), the requirements set out in Chapter III, Section 2, of that Regulation shall be taken into account.

(*) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (OJ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).’.

第104条

对(EU)第168/2013号条例的修订

在第168/2013号条例(欧盟)第22(5)条中，增加以下分段：

“在根据第一小段通过有关属于欧洲议会和理事会条例(EU) 2024/1689(*)所指安全组件的人工智能系统的授权法案时，应考虑到该条例第三章第2节规定的要求。

(*) 欧洲议会和理事会2024年6月13日第(EU) 2024/1689号条例，规定统一规则并修订条例(EC) No 300/2008、(EU) No 167/2013、(EU) No 168/2013、(EU) 2018/858、(EU) 2018/1139和(EU) 2019/2144以及指令2014/90/EU、(EU) 2016/797和(EU) 2020/1828(人工智能法案)(OJ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/ 2024/1689/oj)。”。

第105条

对指令 (EU) 2014/90 的修订

在指令2014/90/EU第8条中，增加以下段落：

“5. 对于属于欧洲议会和理事会条例(EU) 2024/1689(*)所指安全组件的人工智能系统，委员会在根据第1款开展活动以及根据第2款和第3款通过技术规范和测试标准时，应考虑该条例第三章第二节规定的要求。

(*) 欧洲议会和理事会2024年6月13日第(EU) 2024/1689号条例，规定统一规则并修订条例(EC) No 300/2008、(EU) No 167/2013、(EU) No 168/2013、(EU) 2018/858、(EU) 2018/1139和(EU) 2019/2144以及指令2014/90/EU、(EU) 2016/797和(EU) 2020/1828(人工智能法案)(OJ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/ 2024/1689/oj)。”。

第106条

对指令 (EU) 2016/797 的修订

在指令(EU) 2016/797第5条中，增加以下段落：

“12. 在根据第1段通过授权法案以及根据第11段通过实施法案，涉及属于欧洲议会和理事会条例(EU) 2024/1689(*)所指安全组件的人工智能系统时，应考虑到该条例第三章第2节规定的要求。

(*) 欧洲议会和理事会2024年6月13日第(EU) 2024/1689号条例，规定统一规则并修订条例(EC) No 300/2008、(EU) No 167/2013、(EU) No 168/2013、(EU) 2018/858、(EU) 2018/1139和(EU) 2019/2144以及指令2014/90/EU、(EU) 2016/797和(EU) 2020/1828(人工智能法案)(OJ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/ 2024/1689/oj)。”。

Article 107

Amendment to Regulation (EU) 2018/858

In Article 5 of Regulation (EU) 2018/858 the following paragraph is added:

‘4. When adopting delegated acts pursuant to paragraph 3 concerning Artificial Intelligence systems which are safety components within the meaning of Regulation (EU) 2024/1689 of the European Parliament and of the Council (*), the requirements set out in Chapter III, Section 2, of that Regulation shall be taken into account.

(*) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (OJ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).’.

Article 108

Amendments to Regulation (EU) 2018/1139

Regulation (EU) 2018/1139 is amended as follows:

(1) in Article 17, the following paragraph is added:

‘3. Without prejudice to paragraph 2, when adopting implementing acts pursuant to paragraph 1 concerning Artificial Intelligence systems which are safety components within the meaning of Regulation (EU) 2024/1689 of the European Parliament and of the Council (*), the requirements set out in Chapter III, Section 2, of that Regulation shall be taken into account.

(*) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (OJ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).’;

(2) in Article 19, the following paragraph is added:

‘4. When adopting delegated acts pursuant to paragraphs 1 and 2 concerning Artificial Intelligence systems which are safety components within the meaning of Regulation (EU) 2024/1689, the requirements set out in Chapter III, Section 2, of that Regulation shall be taken into account.’;

(3) in Article 43, the following paragraph is added:

‘4. When adopting implementing acts pursuant to paragraph 1 concerning Artificial Intelligence systems which are safety components within the meaning of Regulation (EU) 2024/1689, the requirements set out in Chapter III, Section 2, of that Regulation shall be taken into account.’;

(4) in Article 47, the following paragraph is added:

‘3. When adopting delegated acts pursuant to paragraphs 1 and 2 concerning Artificial Intelligence systems which are safety components within the meaning of Regulation (EU) 2024/1689, the requirements set out in Chapter III, Section 2, of that Regulation shall be taken into account.’;

(5) in Article 57, the following subparagraph is added:

‘When adopting those implementing acts concerning Artificial Intelligence systems which are safety components within the meaning of Regulation (EU) 2024/1689, the requirements set out in Chapter III, Section 2, of that Regulation shall be taken into account.’;

第107条

对(EU) 2018/858号条例的修订

在(EU) 2018/858号法规第5条中，增加以下段落：

“4. 在根据第3段通过授权法案，涉及属于欧洲议会和理事会条例(EU) 2024/1689(*)所指安全组件的人工智能系统时，应考虑到该条例第三章第2节规定的要求。

(*) 欧洲议会和理事会2024年6月13日第(EU) 2024/1689号条例，规定统一规则并修订条例(EC) No 300/2008、(EU) No 167/2013、(EU) No 168/2013、(EU) 2018/858、(EU) 2018/1139和(EU) 2019/2144以及指令2014/90/EU、(EU) 2016/797和(EU) 2020/1828(人工智能法案)(OJ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/ 2024/1689/oj)。”。

第108条

对(EU) 2018/1139号条例的修订

Regulation (EU) 2018/1139 修订如下：

(1) 在第17条中，增加以下段落：

“3. 在不影响第2款的情况下，在根据第1款通过实施法案，涉及属于欧洲议会和理事会条例(EU) 2024/1689(*)所指安全组件的人工智能系统时，应考虑该条例第三章第二节规定的要求。

(*) 欧洲议会和理事会2024年6月13日第(EU) 2024/1689号条例，规定人工智能统一规则并修订条例(EC) No 300/2008、(EU) No 167/2013、(EU) No 168/2013、(EU) 2018/858、(EU) 2018/1139和(EU) 2019/2144以及指令2014/90/EU、(EU) 2016/797和(EU) 2020/1828(人工智能法案)(OJ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj)。”;

(2) 在Article 19中，增加以下段落：

“4. 在根据第1款和第2款通过授权法案，涉及属于条例(EU) 2024/1689所指安全组件的人工智能系统时，应考虑该条例第三章第二节规定的要求。”;

(3) 在Article 43中，增加以下段落：

‘4. 在依据第1款通过有关属于Regulation(EU) 2024/1689所指安全组件的人工智能系统的实施法案时，应考虑到该条例Chapter III, Section 2中规定的要求。’;

(4) 在第47条中，增加以下段落：

“3. 在根据第1款和第2款通过授权法案，涉及属于条例(EU) 2024/1689所指安全组件的人工智能系统时，应考虑该条例第三章第二节规定的要求。”;

(5) 在第57条中，增加以下子段：

‘在通过有关属于Regulation(EU) 2024/1689所指安全组件的人工智能系统的该等实施法案时，应考虑到该条例Chapter III, Section 2中规定的要求。’;

(6) in Article 58, the following paragraph is added:

'3. When adopting delegated acts pursuant to paragraphs 1 and 2 concerning Artificial Intelligence systems which are safety components within the meaning of Regulation (EU) 2024/1689, the requirements set out in Chapter III, Section 2, of that Regulation shall be taken into account.'.

Article 109

Amendment to Regulation (EU) 2019/2144

In Article 11 of Regulation (EU) 2019/2144, the following paragraph is added:

'3. When adopting the implementing acts pursuant to paragraph 2, concerning artificial intelligence systems which are safety components within the meaning of Regulation (EU) 2024/1689 of the European Parliament and of the Council (*), the requirements set out in Chapter III, Section 2, of that Regulation shall be taken into account.

(*) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (OJ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).'.

Article 110

Amendment to Directive (EU) 2020/1828

In Annex I to Directive (EU) 2020/1828 of the European Parliament and of the Council ([58]), the following point is added:

'(68) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (OJ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).'.

Article 111

AI systems already placed on the market or put into service and general-purpose AI models already placed on the marked

1. Without prejudice to the application of Article 5 as referred to in Article 113(3), point (a), AI systems which are components of the large-scale IT systems established by the legal acts listed in Annex X that have been placed on the market or put into service before 2 August 2027 shall be brought into compliance with this Regulation by 31 December 2030.

The requirements laid down in this Regulation shall be taken into account in the evaluation of each large-scale IT system established by the legal acts listed in Annex X to be undertaken as provided for in those legal acts and where those legal acts are replaced or amended.

2. Without prejudice to the application of Article 5 as referred to in Article 113(3), point (a), this Regulation shall apply to operators of high-risk AI systems, other than the systems referred to in paragraph 1 of this Article, that have been placed on the market or put into service before 2 August 2026, only if, as from that date, those systems are subject to significant changes in their designs. In any case, the providers and deployers of high-risk AI systems intended to be used by public authorities shall take the necessary steps to comply with the requirements and obligations of this Regulation by 2 August 2030.

3. Providers of general-purpose AI models that have been placed on the market before 2 August 2025 shall take the necessary steps in order to comply with the obligations laid down in this Regulation by 2 August 2027.

([58]) Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC (OJ L 409, 4.12.2020, p. 1).

(6) 在Article 58中，增加以下段落：

"3. 在根据第1款和第2款通过授权法案，涉及属于条例(EU) 2024/1689所指安全组件的人工智能系统时，应考虑该条例第三章第二节规定的要求。"。

第109条

对条例 (EU) 2019/2144 的修订

在(EU) 2019/2144号法规第11条中，增加以下段落：

"3. 在根据第2款通过实施法案，涉及属于欧洲议会和理事会条例(EU) 2024/1689(*)所指安全组件的人工智能系统时，应考虑该条例第三章第二节规定的要求。

(*) 欧洲议会和理事会2024年6月13日第(EU) 2024/1689号条例，规定统一规则并修订条例(EC) No 300/2008、(EU) No 167/2013、(EU) No 168/2013、(EU) 2018/858、(EU) 2018/1139和(EU) 2019/2144以及指令2014/90/EU、(EU) 2016/797和(EU) 2020/1828(人工智能法案)(OJ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/ 2024/1689/oj)。"。

第110条

对指令 (EU) 2020/1828 的修订

在欧洲议会和理事会指令(EU) 2020/1828(58)的附件一中，增加以下条目：

(68) 欧洲议会和理事会2024年6月13日关于制定统一规则的第(EU) 2024/1689号条例规则并修订条例(EC) No 300/2008、(EU) No 167/2013、(EU) No 168/2013、(EU) 2018/858、(EU) 2018/1139和(EU) 2019/2144以及指令2014/90/EU、(EU) 2016/797和(EU) 2020/1828(人工智能法案)(OJ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/ 2024/1689/oj)。"。

第111条

已投放市场或已投入服务的人工智能系统以及已投放的通用人工智能模型

标记

1. 在不影响第113(3)条第(a)点所述第5条适用的情况下，作为附件十所列法律法案建立的大规模IT系统组件的人工智能系统，如在2027年8月2日之前已投放市场或投入使用，应于2030年12月31日前符合本条例。

在评估附件十所列法律法案所建立的各大规模IT系统时，应按照这些法律法案的规定并在其被替换或修订时，考虑本条例规定的要求。

2. 在不影响第113(3)条第(a)点所述第5条适用的情况下，本条例仅自2026年8月2日起，对已在该日期前投放市场或投入使用的、本条第1款所述系统以外的高风险人工智能系统的运营者适用，且仅限于这些系统自该日期起其设计发生重大变更的情形。无论如何，拟由公共机关使用的高风险人工智能系统的提供者和部署者应于2030年8月2日前采取必要步骤，遵守本条例的要求和义务。

3. 在2025年8月2日之前已投放市场的通用人工智能模型的提供者，应采取必要步骤，以便在2027年8月2日之前遵守本条例规定的义务。

(58) 欧洲议会和理事会2020年11月25日关于为保护消费者集体利益而提起代表诉讼并废止Directive 2009/22/EC的Directive (EU) 2020/1828(OJ L 409, 4.12.2020, p.1)。

Article 112

Evaluation and review

1. The Commission shall assess the need for amendment of the list set out in Annex III and of the list of prohibited AI practices laid down in Article 5, once a year following the entry into force of this Regulation, and until the end of the period of the delegation of power laid down in Article 97. The Commission shall submit the findings of that assessment to the European Parliament and the Council.

2. By 2 August 2028 and every four years thereafter, the Commission shall evaluate and report to the European Parliament and to the Council on the following:

(a) the need for amendments extending existing area headings or adding new area headings in Annex III;

(b) amendments to the list of AI systems requiring additional transparency measures in Article 50;

(c) amendments enhancing the effectiveness of the supervision and governance system.

3. By 2 August 2029 and every four years thereafter, the Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council. The report shall include an assessment with regard to the structure of enforcement and the possible need for a Union agency to resolve any identified shortcomings. On the basis of the findings, that report shall, where appropriate, be accompanied by a proposal for amendment of this Regulation. The reports shall be made public.

4. The reports referred to in paragraph 2 shall pay specific attention to the following:

(a) the status of the financial, technical and human resources of the national competent authorities in order to effectively perform the tasks assigned to them under this Regulation;

(b) the state of penalties, in particular administrative fines as referred to in Article 99(1), applied by Member States for infringements of this Regulation;

(c) adopted harmonised standards and common specifications developed to support this Regulation;

(d) the number of undertakings that enter the market after the entry into application of this Regulation, and how many of them are SMEs.

5. By 2 August 2028, the Commission shall evaluate the functioning of the AI Office, whether the AI Office has been given sufficient powers and competences to fulfil its tasks, and whether it would be relevant and needed for the proper implementation and enforcement of this Regulation to upgrade the AI Office and its enforcement competences and to increase its resources. The Commission shall submit a report on its evaluation to the European Parliament and to the Council.

6. By 2 August 2028 and every four years thereafter, the Commission shall submit a report on the review of the progress on the development of standardisation deliverables on the energy-efficient development of general-purpose AI models, and asses the need for further measures or actions, including binding measures or actions. The report shall be submitted to the European Parliament and to the Council, and it shall be made public.

7. By 2 August 2028 and every three years thereafter, the Commission shall evaluate the impact and effectiveness of voluntary codes of conduct to foster the application of the requirements set out in Chapter III, Section 2 for AI systems other than high-risk AI systems and possibly other additional requirements for AI systems other than high-risk AI systems, including as regards environmental sustainability.

8. For the purposes of paragraphs 1 to 7, the Board, the Member States and national competent authorities shall provide the Commission with information upon its request and without undue delay.

9. In carrying out the evaluations and reviews referred to in paragraphs 1 to 7, the Commission shall take into account the positions and findings of the Board, of the European Parliament, of the Council, and of other relevant bodies or sources.

第112条

评估与审查

1. 委员会应在本条例生效后每年一次评估是否需要修订附件三所列清单和第5条规定的禁止的人工智能实践清单，直至第97条规定的授权期限结束。委员会应向欧洲议会和理事会提交该评估的结论。

2. 委员会应于2028年8月2日前及此后每四年评估下列事项并向欧洲议会和理事会报告：

(a) 是否需要修订以扩展附件三中现有领域标题或增加新的领域标题；

(b) 对第50条中需要额外透明度措施的人工智能系统清单的修订；

(c) 增强监督与治理体系有效性的修正案。

3. 委员会应于2029年8月2日之前及此后每四年向欧洲议会和理事会提交一份关于本条例评估与审查的报告。该报告应包括对执法结构以及是否可能需要设立一个联盟机构以解决任何已查明缺陷的评估。基于评估结论，该报告应在适当情况下附有对本条例的修订提案。报告应予以公开。

4. 第2款所指报告应特别关注以下事项：

(a) 国家主管机关为有效履行本条例赋予的任务而具备的财政、技术和人力资源状况；

(b) 成员国针对违反本条例的行为所施加的处罚情况，特别是第99(1)条所指的行政罚款；

(c) 为支持本条例而制定的已采纳的协调标准和通用规范；

(d) 本条例开始适用后进入市场的企业数量，以及其中有多少是中小企业。

5. 到2028年8月2日，委员会应评估人工智能办公室的运作情况、人工智能办公室是否已被赋予足够的权力和权限以履行其任务，以及为妥善实施和执行本条例而升级人工智能办公室及其执行权限并增加其资源是否相关且必要。委员会应向欧洲议会和理事会提交其评估报告。

6. 委员会应于2028年8月2日之前及此后每四年提交一份报告，审查关于通用人工智能模型能效开发标准化交付成果的进展，并评估是否需要进一步措施或行动，包括具有约束力的措施或行动。该报告应提交欧洲议会和理事会，并应予以公开。

7. 到2028年8月2日及此后每三年，委员会应评估自愿行为准则在促进对非高风险人工智能系统适用第三章第2节所规定要求方面的影响和有效性，以及可能对非高风险人工智能系统适用的其他附加要求，包括在环境可持续性方面。

8. 为第1至7款之目的，委员会应要求时，理事会、成员国和国家主管机关应无不当延迟地向委员会提供信息。

9. 在开展第1至7款所指的评估和审查时，委员会应考虑理事会、欧洲议会以及其他相关机构或来源的立场和结论。

10. The Commission shall, if necessary, submit appropriate proposals to amend this Regulation, in particular taking into account developments in technology, the effect of AI systems on health and safety, and on fundamental rights, and in light of the state of progress in the information society.

11. To guide the evaluations and reviews referred to in paragraphs 1 to 7 of this Article, the AI Office shall undertake to develop an objective and participative methodology for the evaluation of risk levels based on the criteria outlined in the relevant Articles and the inclusion of new systems in:

(a) the list set out in Annex III, including the extension of existing area headings or the addition of new area headings in that Annex;

(b) the list of prohibited practices set out in Article 5; and

(c) the list of AI systems requiring additional transparency measures pursuant to Article 50.

12. Any amendment to this Regulation pursuant to paragraph 10, or relevant delegated or implementing acts, which concerns sectoral Union harmonisation legislation listed in Section B of Annex I shall take into account the regulatory specificities of each sector, and the existing governance, conformity assessment and enforcement mechanisms and authorities established therein.

13. By 2 August 2031, the Commission shall carry out an assessment of the enforcement of this Regulation and shall report on it to the European Parliament, the Council and the European Economic and Social Committee, taking into account the first years of application of this Regulation. On the basis of the findings, that report shall, where appropriate, be accompanied by a proposal for amendment of this Regulation with regard to the structure of enforcement and the need for a Union agency to resolve any identified shortcomings.

Article 113

Entry into force and application

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

It shall apply from 2 August 2026.

However:

(a) Chapters I and II shall apply from 2 February 2025;

(b) Chapter III Section 4, Chapter V, Chapter VII and Chapter XII and Article 78 shall apply from 2 August 2025, with the exception of Article 101;

(c) Article 6(1) and the corresponding obligations in this Regulation shall apply from 2 August 2027.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 13 June 2024.

For the European Parliament
The President
R. METSOLA

For the Council
The President
M. MICHEL

10. 委员会应在必要时提交适当的提案以修订本条例，特别是考虑到技术发展、人工智能系统对健康和安全以及对基本权利的影响，并根据信息社会的进展状况。

11. 为指导本条第1至7款所指的评估和审查，人工智能办公室应着手制定一种客观且参与式的方法，用于基于相关条款所列标准评估风险水平，并将新系统纳入：

(a) 附件三所列清单，包括扩展该附件中现有的领域标题或增加新的领域标题；

(b) 第5条所列禁止性做法清单；以及

(c) 依据第50条需要额外透明度措施的人工智能系统清单。

12. 依据第10款对本条例的任何修订，或相关的授权法案或实施法案，凡涉及附件一B节所列的部门欧盟协调立法的，应考虑到每个部门的监管特殊性，以及其中建立的现有治理、合格评定和执法机制及主管机关。

13. 到2031年8月2日，委员会应就本条例的执行情况进行评估，并考虑到本条例最初几年的适用情况，向欧洲议会、理事会和欧洲经济及社会委员会报告。基于评估结果，该报告应酌情附上对本条例的修订提案，涉及执行结构以及是否需要设立一个联盟机构来解决任何已发现的缺陷。

第113条

生效与适用

本 Regulation 应在其在欧盟官方公报上公布之日后第二十天生效。

它自2026年8月2日起适用。

但是：

(a) 第一章和第二章自2025年2月2日起适用；(b) 第三章第4节、第五章、第七章和第十二章以及第78条自2025年8月2日起适用，但第101条除外；

(c) Article 6(1) 及本条例中相应的义务自 2 August 2027 起适用。

本 Regulation 整体具有约束力，并直接适用于所有成员国。

2024年6月13日订于布鲁塞尔。

致欧洲议会
主席
R. 梅措拉

提交理事会
主席
M. 米歇尔

ANNEX I

List of Union harmonisation legislation

Section A. List of Union harmonisation legislation based on the New Legislative Framework

1. Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (OJ L 157, 9.6.2006, p. 24);

2. Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys (OJ L 170, 30.6.2009, p. 1);

3. Directive 2013/53/EU of the European Parliament and of the Council of 20 November 2013 on recreational craft and personal watercraft and repealing Directive 94/25/EC (OJ L 354, 28.12.2013, p. 90);

4. Directive 2014/33/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to lifts and safety components for lifts (OJ L 96, 29.3.2014, p. 251);

5. Directive 2014/34/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to equipment and protective systems intended for use in potentially explosive atmospheres (OJ L 96, 29.3.2014, p. 309);

6. Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC (OJ L 153, 22.5.2014, p. 62);

7. Directive 2014/68/EU of the European Parliament and of the Council of 15 May 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of pressure equipment (OJ L 189, 27.6.2014, p. 164);

8. Regulation (EU) 2016/424 of the European Parliament and of the Council of 9 March 2016 on cableway installations and repealing Directive 2000/9/EC (OJ L 81, 31.3.2016, p. 1);

9. Regulation (EU) 2016/425 of the European Parliament and of the Council of 9 March 2016 on personal protective equipment and repealing Council Directive 89/686/EEC (OJ L 81, 31.3.2016, p. 51);

10. Regulation (EU) 2016/426 of the European Parliament and of the Council of 9 March 2016 on appliances burning gaseous fuels and repealing Directive 2009/142/EC (OJ L 81, 31.3.2016, p. 99);

11. Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117, 5.5.2017, p. 1);

12. Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on *in vitro* diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (OJ L 117, 5.5.2017, p. 176).

Section B. List of other Union harmonisation legislation

13. Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (OJ L 97, 9.4.2008, p. 72);

14. Regulation (EU) No 168/2013 of the European Parliament and of the Council of 15 January 2013 on the approval and market surveillance of two- or three-wheel vehicles and quadricycles (OJ L 60, 2.3.2013, p. 52);

15. Regulation (EU) No 167/2013 of the European Parliament and of the Council of 5 February 2013 on the approval and market surveillance of agricultural and forestry vehicles (OJ L 60, 2.3.2013, p. 1);

附件一

欧盟统一化立法清单

A节.基于新立法框架的欧盟协调立法清单

1. 欧洲议会和理事会2006年5月17日关于机械的指令2006/42/EC，并修订指令95/16/EC(OJ L 157, 9.6.2006, p.24);

2. 欧洲议会和理事会2009年6月18日关于玩具安全的指令2009/48/EC(OJ L 170,2009年6月30日，第1页);

3. 欧洲议会和理事会2013年11月20日关于休闲船只和个人水上摩托并废止第94/25/EC号指令的第2013/53/EU号指令(OJ L 354, 28.12.2013, p.90);

4. 欧洲议会和理事会2014年2月26日关于成员国有关电梯和电梯安全组件的法律协调的第2014/33/EU号指令(OJ L 96, 29.3.2014, p.251);

5. 欧洲议会和理事会2014年2月26日关于统一成员国有关拟用于潜在爆炸性环境的设备和防护系统的法律的指令2014/34/EU(OJ L 96, 29.3.2014, p.309);

6. 欧洲议会和理事会2014年4月16日关于统一成员国有关无线电设备在市场上提供的法律并废除指令1999/5/EC的指令2014/53/EU(OJ L 153, 22.5.2014, p.62);

7. 欧洲议会和理事会2014年5月15日关于协调成员国有关压力设备投放市场法律的指令2014/68/EU(OJ L 189, 27.6.2014, p.164);

8. 欧洲议会和理事会2016年3月9日关于索道装置并废止指令2000/9/EC的条例(EU)2016/424(OJ L 81,2016年3月31日，第1页);

9. 欧洲议会和理事会2016年3月9日关于个人防护装备并废止理事会指令89/686/EEC的条例(EU)2016/425(OJ L 81,2016年3月31日，第51页);

10. 欧洲议会和理事会2016年3月9日关于燃烧气体燃料的器具并废止指令2009/142/EC的条例(EU)2016/426(OJ L 81,2016年3月31日，第99页);

11. 欧洲议会和理事会2017年4月5日关于医疗器械的第(EU) 2017/745号条例，修订第2001/83/EC号指令、第(EC) No 178/2002号条例和第(EC) No 1223/2009号条例，并废止理事会第90/385/EEC号和第93/42/EEC号指令(OJ L 117, 5.5.2017, p.1);

12. 欧洲议会和理事会2017年4月5日关于体外诊断医疗器械并废止指令98/79/EC及委员会决定2010/227/EU的(EU) 2017/746号条例(OJ L 117, 5.5.2017, p.176)。

B部分.其他联盟统一立法清单

13. 欧洲议会和理事会2008年3月11日关于民用航空安保领域共同规则并废止第(EC) No 2320/2002号条例的第(EC) No 300/2008号条例(OJ L 97, 9.4.2008, p.72);

14. 欧洲议会和理事会2013年1月15日关于两轮或三轮车辆和四轮车批准与市场监督的第168/2013号条例(EU)(OJ L 60, 2.3.2013, p.52);

15. 欧洲议会和理事会2013年2月5日关于农林车辆认证和市场监督的条例(EU)第167/2013号(OJ L 60,2013年3月2日，第1页);

16. Directive 2014/90/EU of the European Parliament and of the Council of 23 July 2014 on marine equipment and repealing Council Directive 96/98/EC (OJ L 257, 28.8.2014, p. 146);

17. Directive (EU) 2016/797 of the European Parliament and of the Council of 11 May 2016 on the interoperability of the rail system within the European Union (OJ L 138, 26.5.2016, p. 44);

18. Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC (OJ L 151, 14.6.2018, p. 1);

19. Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166 (OJ L 325, 16.12.2019, p. 1);

20. Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (OJ L 212, 22.8.2018, p. 1), in so far as the design, production and placing on the market of aircrafts referred to in Article 2(1), points (a) and (b) thereof, where it concerns unmanned aircraft and their engines, propellers, parts and equipment to control them remotely, are concerned.

16. 欧洲议会和理事会2014年7月23日关于船用设备并废止理事会第96/98/EC号指令的第2014/90/EU号指令(OJ L 257, 28.8.2014, p.146);

17. 欧洲议会和理事会2016年5月11日关于欧洲联盟内铁路系统互操作性的指令(EU)2016/797(OJ L 138,2016年5月26日，第44页);

18. 欧洲议会和理事会2018年5月30日关于机动车及其挂车以及用于此类车辆的系统、组件和独立技术单元的批准和市场监督，修订(EC) No 715/2007号条例和(EC) No 595/2009号条例并废止2007/46/EC指令的(EU) 2018/858号条例(OJ L 151, 14.6.2018, p.1);

19. 欧洲议会和理事会2019年11月27日关于机动车及其挂车以及旨在用于此类车辆的系统、部件和独立技术单元在一般安全性和车辆乘员及弱势道路使用者保护方面的型式认证要求的条例(EU) 2019/2144，修订欧洲议会和理事会条例(EU) 2018/858并废止欧洲议会和理事会条例(EC)第78/2009号、(EC)第79/2009号和(EC)第661/2009号以及委员会条例(EC)第631/2009号、(EU)第406/2010号、(EU)第672/2010号、(EU)第1003/2010号、(EU)第1005/2010号、(EU)第1008/2010号、(EU)第1009/2010号、(EU)第19/2011号、(EU)第109/2011号、(EU)第458/2011号、(EU)第65/2012号、(EU)第130/2012号、(EU)第347/2012号、(EU)第351/2012号、(EU)第1230/2012号和(EU) 2015/166号（OJ L 325，2019年12月16日，第1页）；

20. 欧洲议会和理事会2018年7月4日关于民用航空领域共同规则并设立欧盟航空安全局、修订欧洲议会和理事会第(EC) No 2111/2005号条例、第(EC) No 1008/2008号条例、第(EU) No 996/2010号条例、第(EU) No 376/2014号条例及第2014/30/EU号和第2014/53/EU号指令、并废止欧洲议会和理事会第(EC) No 552/2004号条例和第(EC) No 216/2008号条例及理事会第(EEC) No 3922/91号条例的第(EU) 2018/1139号条例(OJ L 212, 22.8.2018, p.1)，就其第2(1)条(a)项和(b)项所述航空器的设计、生产和投放市场而言，涉及无人驾驶航空器及其发动机、螺旋桨、部件和远程控制设备。

ANNEX II

List of criminal offences referred to in Article 5(1), first subparagraph, point (h)(iii)

Criminal offences referred to in Article 5(1), first subparagraph, point (h)(iii):

— terrorism,

— trafficking in human beings,

— sexual exploitation of children, and child pornography,

— illicit trafficking in narcotic drugs or psychotropic substances,

— illicit trafficking in weapons, munitions or explosives,

— murder, grievous bodily injury,

— illicit trade in human organs or tissue,

— illicit trafficking in nuclear or radioactive materials,

— kidnapping, illegal restraint or hostage-taking,

— crimes within the jurisdiction of the International Criminal Court,

— unlawful seizure of aircraft or ships,

— rape,

— environmental crime,

— organised or armed robbery,

— sabotage,

— participation in a criminal organisation involved in one or more of the offences listed above.

附件二

第5(1)条第一项第(h)点第(iii)目所指的刑事犯罪清单

第5(1)条第一项第(h)点第(iii)目所指的刑事犯罪：- 恐怖主义，

- 人口贩运，

- 对儿童的性剥削和儿童色情制品，- 非法贩运麻醉药品或精神药物，- 非法贩运武器、弹药或爆炸物，- 谋杀、严重身体伤害，

- 人体器官或组织的非法交易，- 非法贩运核材料或放射性材料，- 绑架、非法拘禁或劫持人质，- 国际刑事法院管辖范围内的犯罪，- 非法劫持航空器或船舶，

— 强奸，

- 环境犯罪，

- 有组织抢劫或武装抢劫，

— 破坏活动，

- 参与从事上述一项或多项犯罪的犯罪组织。

ANNEX III

High-risk AI systems referred to in Article 6(2)

High-risk AI systems pursuant to Article 6(2) are the AI systems listed in any of the following areas:

1. Biometrics, in so far as their use is permitted under relevant Union or national law:

   (a) remote biometric identification systems.

   This shall not include AI systems intended to be used for biometric verification the sole purpose of which is to confirm that a specific natural person is the person he or she claims to be;

   (b) AI systems intended to be used for biometric categorisation, according to sensitive or protected attributes or characteristics based on the inference of those attributes or characteristics;

   (c) AI systems intended to be used for emotion recognition.

2. Critical infrastructure: AI systems intended to be used as safety components in the management and operation of critical digital infrastructure, road traffic, or in the supply of water, gas, heating or electricity.

3. Education and vocational training:

   (a) AI systems intended to be used to determine access or admission or to assign natural persons to educational and vocational training institutions at all levels;

   (b) AI systems intended to be used to evaluate learning outcomes, including when those outcomes are used to steer the learning process of natural persons in educational and vocational training institutions at all levels;

   (c) AI systems intended to be used for the purpose of assessing the appropriate level of education that an individual will receive or will be able to access, in the context of or within educational and vocational training institutions at all levels;

   (d) AI systems intended to be used for monitoring and detecting prohibited behaviour of students during tests in the context of or within educational and vocational training institutions at all levels.

4. Employment, workers' management and access to self-employment:

   (a) AI systems intended to be used for the recruitment or selection of natural persons, in particular to place targeted job advertisements, to analyse and filter job applications, and to evaluate candidates;

   (b) AI systems intended to be used to make decisions affecting terms of work-related relationships, the promotion or termination of work-related contractual relationships, to allocate tasks based on individual behaviour or personal traits or characteristics or to monitor and evaluate the performance and behaviour of persons in such relationships.

5. Access to and enjoyment of essential private services and essential public services and benefits:

   (a) AI systems intended to be used by public authorities or on behalf of public authorities to evaluate the eligibility of natural persons for essential public assistance benefits and services, including healthcare services, as well as to grant, reduce, revoke, or reclaim such benefits and services;

   (b) AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score, with the exception of AI systems used for the purpose of detecting financial fraud;

   (c) AI systems intended to be used for risk assessment and pricing in relation to natural persons in the case of life and health insurance;

附件三

第6(2)条所述高风险人工智能系统

依据第6(2)条的高风险人工智能系统是下列任一领域所列的人工智能系统：

1. 生物特征识别，只要其使用根据相关联盟或国家法律被允许：

   (a) 远程生物识别系统。

   这不应包括旨在用于生物特征验证的人工智能系统，其唯一目的是确认某一特定自然人是其声称的人；

   (b) 旨在用于生物特征分类的人工智能系统，根据敏感或受保护的属性或特征，基于对这些属性或特征的推断；

   (c) 用于情感识别的AI系统。

2. 关键基础设施：旨在用作关键数字基础设施、道路交通的管理和运营或水、燃气、供暖或电力供应中的安全组件的人工智能系统。

3. 教育与职业培训：

   (a) 旨在用于确定各级教育和职业培训机构的准入或录取或分配自然人的AI系统；

   (b) 旨在用于评估学习成果的人工智能系统，包括当这些成果被用于引导各级教育和职业培训机构中自然人的学习过程时；

   (c) 旨在用于评估个人在各级教育和职业培训机构背景下或范围内将接受或能够获得的适当教育水平的人工智能系统；

   (d) 旨在用于在各级教育和职业培训机构背景下或范围内监测和检测学生在测试期间的禁止行为的人工智能系统。

4. 就业、劳动者管理与自雇准入：

   (a) 拟用于自然人招聘或选拔的人工智能系统，特别是用于投放定向招聘广告、分析和筛选求职申请以及评估候选人；

   (b) 拟用于作出影响工作相关关系条款、工作相关合同关系的晋升或终止的决定，基于个人行为或个人特质或特征分配任务，或监测和评估此类关系中人员绩效和行为的人工智能系统。

5. 获取和享有基本私人服务和基本公共服务及福利：

   (a) 拟由公共当局或代表公共当局使用，以评估自然人获得基本公共援助福利和服务(包括医疗保健服务)的资格，以及授予、减少、撤销或追回此类福利和服务的人工智能系统；

   (b) 拟用于评估自然人信用worthiness或确定其信用评分的人工智能系统，但用于检测金融欺诈目的的人工智能系统除外；

   (c) 拟用于人寿和健康保险中与自然人相关的风险评估和定价的人工智能系统；

(d) AI systems intended to evaluate and classify emergency calls by natural persons or to be used to dispatch, or to establish priority in the dispatching of, emergency first response services, including by police, firefighters and medical aid, as well as of emergency healthcare patient triage systems.

6. Law enforcement, in so far as their use is permitted under relevant Union or national law:

(a) AI systems intended to be used by or on behalf of law enforcement authorities, or by Union institutions, bodies, offices or agencies in support of law enforcement authorities or on their behalf to assess the risk of a natural person becoming the victim of criminal offences;

(b) AI systems intended to be used by or on behalf of law enforcement authorities or by Union institutions, bodies, offices or agencies in support of law enforcement authorities as polygraphs or similar tools;

(c) AI systems intended to be used by or on behalf of law enforcement authorities, or by Union institutions, bodies, offices or agencies, in support of law enforcement authorities to evaluate the reliability of evidence in the course of the investigation or prosecution of criminal offences;

(d) AI systems intended to be used by law enforcement authorities or on their behalf or by Union institutions, bodies, offices or agencies in support of law enforcement authorities for assessing the risk of a natural person offending or re-offending not solely on the basis of the profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680, or to assess personality traits and characteristics or past criminal behaviour of natural persons or groups;

(e) AI systems intended to be used by or on behalf of law enforcement authorities or by Union institutions, bodies, offices or agencies in support of law enforcement authorities for the profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 in the course of the detection, investigation or prosecution of criminal offences.

7. Migration, asylum and border control management, in so far as their use is permitted under relevant Union or national law:

(a) AI systems intended to be used by or on behalf of competent public authorities or by Union institutions, bodies, offices or agencies as polygraphs or similar tools;

(b) AI systems intended to be used by or on behalf of competent public authorities or by Union institutions, bodies, offices or agencies to assess a risk, including a security risk, a risk of irregular migration, or a health risk, posed by a natural person who intends to enter or who has entered into the territory of a Member State;

(c) AI systems intended to be used by or on behalf of competent public authorities or by Union institutions, bodies, offices or agencies to assist competent public authorities for the examination of applications for asylum, visa or residence permits and for associated complaints with regard to the eligibility of the natural persons applying for a status, including related assessments of the reliability of evidence;

(d) AI systems intended to be used by or on behalf of competent public authorities, or by Union institutions, bodies, offices or agencies, in the context of migration, asylum or border control management, for the purpose of detecting, recognising or identifying natural persons, with the exception of the verification of travel documents.

8. Administration of justice and democratic processes:

(a) AI systems intended to be used by a judicial authority or on their behalf to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts, or to be used in a similar way in alternative dispute resolution;

(d) 拟用于评估和分类自然人紧急呼叫的人工智能系统，或用于调度或确定紧急第一响应服务(包括警察、消防员和医疗援助)调度优先级的人工智能系统，以及紧急医疗保健患者分诊系统。

6. 执法，只要相关欧盟或国家法律允许其使用：

(a) 拟由执法当局或代表执法当局使用，或由联盟机构、机关、办事处或团体为支持执法当局或代表其使用，以评估自然人成为刑事犯罪受害者风险的人工智能系统；

(b) 拟由执法当局或代表执法当局使用，或由联盟机构、机关、办事处或团体为支持执法当局使用，作为测谎仪或类似工具的人工智能系统；

(c) 拟由执法当局或代表执法当局使用，或由联盟机构、机关、办事处或团体为支持执法当局使用，在刑事犯罪调查或起诉过程中评估证据可靠性的人工智能系统；

(d) 拟由执法当局或代表执法当局使用，或由联盟机构、机关、办事处或团体为支持执法当局使用，用于评估自然人犯罪或再次犯罪风险(不仅基于 Directive (EU) 2016/680 第 3(4) 条所述的自然人画像)，或评估自然人或群体的人格特质和特征或过往犯罪行为的人工智能系统；

(e) 拟由执法当局或代表执法当局使用，或由联盟机构、机关、办事处或团体为支持执法当局使用，在刑事犯罪侦查、调查或起诉过程中用于 Directive (EU) 2016/680 第 3(4) 条所述的自然人画像的人工智能系统。

7. 移民、庇护和边境管制管理，只要其使用根据相关联盟或国家法律被允许：

(a) 拟由主管公共当局或代表主管公共当局使用，或由联盟机构、机关、办事处或团体使用，作为测谎仪或类似工具的人工智能系统；

(b) 拟由主管公共当局或代表主管公共当局使用，或由联盟机构、机关、办事处或团体使用，以评估意图进入或已进入成员国领土的自然人所构成的风险，包括安全风险、非正常移民风险或健康风险的人工智能系统；

(c) 拟由主管公共当局或代表主管公共当局使用，或由联盟机构、机关、办事处或团体使用，以协助主管公共当局审查庇护、签证或居留许可申请及相关申诉(涉及申请身份的自然人的资格)，包括对证据可靠性的相关评估的人工智能系统；

(d) 拟由主管公共当局或代表主管公共当局使用，或由联盟机构、机关、办事处或团体使用，在移民、庇护或边境管制管理背景下，用于检测、识别或确认自然人身份的人工智能系统，但旅行证件核验除外。

8. 司法行政与民主进程：

(a) 拟由司法机关或代表司法机关使用，以协助司法机关研究和解释事实与法律并将法律适用于具体事实集合，或在替代性争议解决中以类似方式使用的人工智能系统；

(b) AI systems intended to be used for influencing the outcome of an election or referendum or the voting behaviour of natural persons in the exercise of their vote in elections or referenda. This does not include AI systems to the output of which natural persons are not directly exposed, such as tools used to organise, optimise or structure political campaigns from an administrative or logistical point of view.

(b) 旨在用于影响选举或全民投票结果，或影响自然人在选举或全民投票中行使投票权时的投票行为的人工智能系统。这不包括自然人不会直接接触其输出的人工智能系统，例如用于从行政或后勤角度组织、优化或构建政治竞选活动的工具。

ANNEX IV

Technical documentation referred to in Article 11(1)

The technical documentation referred to in Article 11(1) shall contain at least the following information, as applicable to the relevant AI system:

1. A general description of the AI system including:

   (a) its intended purpose, the name of the provider and the version of the system reflecting its relation to previous versions;

   (b) how the AI system interacts with, or can be used to interact with, hardware or software, including with other AI systems, that are not part of the AI system itself, where applicable;

   (c) the versions of relevant software or firmware, and any requirements related to version updates;

   (d) the description of all the forms in which the AI system is placed on the market or put into service, such as software packages embedded into hardware, downloads, or APIs;

   (e) the description of the hardware on which the AI system is intended to run;

   (f) where the AI system is a component of products, photographs or illustrations showing external features, the marking and internal layout of those products;

   (g) a basic description of the user-interface provided to the deployer;

   (h) instructions for use for the deployer, and a basic description of the user-interface provided to the deployer, where applicable;

2. A detailed description of the elements of the AI system and of the process for its development, including:

   (a) the methods and steps performed for the development of the AI system, including, where relevant, recourse to pre-trained systems or tools provided by third parties and how those were used, integrated or modified by the provider;

   (b) the design specifications of the system, namely the general logic of the AI system and of the algorithms; the key design choices including the rationale and assumptions made, including with regard to persons or groups of persons in respect of who, the system is intended to be used; the main classification choices; what the system is designed to optimise for, and the relevance of the different parameters; the description of the expected output and output quality of the system; the decisions about any possible trade-off made regarding the technical solutions adopted to comply with the requirements set out in Chapter III, Section 2;

   (c) the description of the system architecture explaining how software components build on or feed into each other and integrate into the overall processing; the computational resources used to develop, train, test and validate the AI system;

   (d) where relevant, the data requirements in terms of datasheets describing the training methodologies and techniques and the training data sets used, including a general description of these data sets, information about their provenance, scope and main characteristics; how the data was obtained and selected; labelling procedures (e.g. for supervised learning), data cleaning methodologies (e.g. outliers detection);

   (e) assessment of the human oversight measures needed in accordance with Article 14, including an assessment of the technical measures needed to facilitate the interpretation of the outputs of AI systems by the deployers, in accordance with Article 13(3), point (d);

   (f) where applicable, a detailed description of pre-determined changes to the AI system and its performance, together with all the relevant information related to the technical solutions adopted to ensure continuous compliance of the AI system with the relevant requirements set out in Chapter III, Section 2;

   (g) the validation and testing procedures used, including information about the validation and testing data used and their main characteristics; metrics used to measure accuracy, robustness and compliance with other relevant requirements set out in Chapter III, Section 2, as well as potentially discriminatory impacts; test logs and all test reports dated and signed by the responsible persons, including with regard to pre-determined changes as referred to under point (f);

附件四

第11(1)条所指的技术文档

第11(1)条所述技术文档应至少包含以下信息，视适用于以下情况而定：
相关AI系统：

1. AI 系统的一般描述，包括：

   (a) 其预期用途、提供者的名称以及反映其与先前版本关系的系统版本；

   (b) 人工智能系统如何与不属于该人工智能系统本身的硬件或软件(包括与其他人工智能系统)交互或可用于交互(如适用)；

   (c) 相关软件或固件的版本，以及与版本更新相关的任何要求；

   (d) 对人工智能系统投放市场或投入使用的所有形式的描述，例如嵌入硬件的软件包、下载或API;

   (e) AI 系统预期运行的硬件描述；

   (f) 若人工智能系统是产品的组件，则展示这些产品外部特征、标记和内部布局的照片或插图；

   (g) 向部署者提供的用户界面的基本描述；

   (h) 面向部署者的使用说明，以及对提供给部署者的用户界面的基本描述(如适用);

2. 对人工智能系统要素及其开发过程的详细描述，包括：

   (a) 为开发人工智能系统所执行的方法和步骤，包括在相关情况下使用第三方提供的预训练系统或工具，以及提供者如何使用、集成或修改这些预训练系统或工具；

   (b) 系统的设计规格，即人工智能系统和算法的一般逻辑；关键设计选择，包括所依据的理由和假设，包括关于系统预期使用所针对的人员或人员群体；主要分类选择；系统设计优化的目标，以及不同参数的相关性；系统预期输出和输出质量的描述；关于为遵守Chapter III, Section 2中规定的要求而采用的技术解决方案所作的任何可能权衡的决定；

   (c) 对系统架构的描述，说明软件组件如何相互构建或相互输入并集成到整体处理中；用于开发、训练、测试和验证人工智能系统的计算资源；

   (d) 在相关情况下，以数据表形式说明的数据要求，描述训练方法和技术以及所使用的训练数据集，包括对这些数据集的一般描述、关于其来源、范围和主要特征的信息；数据如何获取和选择；标注程序(例如用于监督学习)、数据清洗方法(例如异常值检测)；

   (e) 根据第14条对所需人类监督措施的评估，包括根据第13(3)条(d)点对便于部署者解释人工智能系统输出所需技术措施的评估；

   (f) 如适用，对人工智能系统及其性能的预定变更的详细描述，以及为确保人工智能系统持续符合第三章第2节所列相关要求而采用的技术解决方案的所有相关信息；

   (g) 所使用的验证和测试程序，包括关于所使用的验证和测试数据及其主要特征的信息；用于衡量准确性、稳健性和符合第三章第2节所列其他相关要求的指标，以及潜在的歧视性影响；由负责人注明日期并签名的测试日志和所有测试报告，包括关于(f)点所述预定变更的测试日志和测试报告；

(h) cybersecurity measures put in place;

3. Detailed information about the monitoring, functioning and control of the AI system, in particular with regard to: its capabilities and limitations in performance, including the degrees of accuracy for specific persons or groups of persons on which the system is intended to be used and the overall expected level of accuracy in relation to its intended purpose; the foreseeable unintended outcomes and sources of risks to health and safety, fundamental rights and discrimination in view of the intended purpose of the AI system; the human oversight measures needed in accordance with Article 14, including the technical measures put in place to facilitate the interpretation of the outputs of AI systems by the deployers; specifications on input data, as appropriate;

4. A description of the appropriateness of the performance metrics for the specific AI system;

5. A detailed description of the risk management system in accordance with Article 9;

6. A description of relevant changes made by the provider to the system through its lifecycle;

7. A list of the harmonised standards applied in full or in part the references of which have been published in the *Official Journal of the European Union*; where no such harmonised standards have been applied, a detailed description of the solutions adopted to meet the requirements set out in Chapter III, Section 2, including a list of other relevant standards and technical specifications applied;

8. A copy of the EU declaration of conformity referred to in Article 47;

9. A detailed description of the system in place to evaluate the AI system performance in the post-market phase in accordance with Article 72, including the post-market monitoring plan referred to in Article 72(3).

(h) 已实施的网络安全措施；

3. 关于人工智能系统的监测、运行和控制的详细信息，特别是关于：其在性能方面的能力和局限性，包括系统预期使用所针对的特定人员或人员群体的准确性程度，以及与其预期目的相关的总体预期准确性水平；鉴于人工智能系统的预期目的，可预见的非预期结果以及健康和安全、基本权利和歧视方面的风险来源；根据Article 14所需的人类监督措施，包括为便于部署者解释人工智能系统输出而采取的技术措施；酌情关于输入数据的规格；

4. 性能指标对特定人工智能系统适当性的描述；

5. 根据第9条对风险管理体系的详细描述；

6. 提供者在系统生命周期内对系统所作相关变更的描述；

7. 已全部或部分应用且其参考文献已在欧盟官方公报上发布的协调标准清单；若未应用此类协调标准，则详细描述为满足第三章第2节所列要求而采用的解决方案，包括所应用的其他相关标准和技术规范的清单；

8. 第47条所指的欧盟符合性声明副本；

9. 对根据第72条在上市后阶段评估人工智能系统性能的系统的详细描述，包括第72(3)条所述上市后监测计划。

ANNEX V

EU declaration of conformity

The EU declaration of conformity referred to in Article 47, shall contain all of the following information:

1. AI system name and type and any additional unambiguous reference allowing the identification and traceability of the AI system;
2. The name and address of the provider or, where applicable, of their authorised representative;
3. A statement that the EU declaration of conformity referred to in Article 47 is issued under the sole responsibility of the provider;
4. A statement that the AI system is in conformity with this Regulation and, if applicable, with any other relevant Union law that provides for the issuing of the EU declaration of conformity referred to in Article 47;
5. Where an AI system involves the processing of personal data, a statement that that AI system complies with Regulations (EU) 2016/679 and (EU) 2018/1725 and Directive (EU) 2016/680;
6. References to any relevant harmonised standards used or any other common specification in relation to which conformity is declared;
7. Where applicable, the name and identification number of the notified body, a description of the conformity assessment procedure performed, and identification of the certificate issued;
8. The place and date of issue of the declaration, the name and function of the person who signed it, as well as an indication for, or on behalf of whom, that person signed, a signature.

附件五

欧盟符合性声明

第47条所述欧盟符合性声明应包含以下所有信息：

1. 人工智能系统名称和类型，以及任何有助于识别和追溯该人工智能系统的额外明确参考信息；
2. 提供者或(如适用)其授权代表的名称和地址；
3. 声明第47条所述的欧盟符合性声明由提供者单独负责发布；
4. 声明人工智能系统符合本条例，并在适用情况下符合规定发布第47条所述欧盟符合性声明的任何其他相关欧盟法律；
5. 若人工智能系统涉及个人数据处理，声明该人工智能系统符合条例(EU) 2016/679和(EU) 2018/1725以及指令(EU) 2016/680;
6. 引用所使用的任何相关协调标准或据以声明符合性的任何其他通用规范；
7. 如适用，公告机构的名称和识别编号、所执行合格评定程序的描述以及所签发证书的标识；
8. 声明的签发地点和日期、签署人的姓名和职务，以及表明该人代表谁或为谁签署的说明、签名。

ANNEX VI

Conformity assessment procedure based on internal control

1. The conformity assessment procedure based on internal control is the conformity assessment procedure based on points 2, 3 and 4.
2. The provider verifies that the established quality management system is in compliance with the requirements of Article 17.
3. The provider examines the information contained in the technical documentation in order to assess the compliance of the AI system with the relevant essential requirements set out in Chapter III, Section 2.
4. The provider also verifies that the design and development process of the AI system and its post-market monitoring as referred to in Article 72 is consistent with the technical documentation.

附件六

基于内部控制的合格评定程序

1. 基于内部控制的合格评定程序是基于第2、3和4点的合格评定程序。
2. 提供者验证所建立的质量管理体系符合第17条的要求。
3. 提供者审查技术文档中包含的信息，以评估人工智能系统是否符合第三章第2节所列相关基本要求。
4. 提供者还验证人工智能系统的设计和开发过程及其第72条所述上市后监测与技术文档一致。

ANNEX VII

Conformity based on an assessment of the quality management system and an assessment of the technical documentation

1. Introduction

Conformity based on an assessment of the quality management system and an assessment of the technical documentation is the conformity assessment procedure based on points 2 to 5.

2. Overview

The approved quality management system for the design, development and testing of AI systems pursuant to Article 17 shall be examined in accordance with point 3 and shall be subject to surveillance as specified in point 5. The technical documentation of the AI system shall be examined in accordance with point 4.

3. Quality management system

3.1. The application of the provider shall include:

(a) the name and address of the provider and, if the application is lodged by an authorised representative, also their name and address;

(b) the list of AI systems covered under the same quality management system;

(c) the technical documentation for each AI system covered under the same quality management system;

(d) the documentation concerning the quality management system which shall cover all the aspects listed under Article 17;

(e) a description of the procedures in place to ensure that the quality management system remains adequate and effective;

(f) a written declaration that the same application has not been lodged with any other notified body.

3.2. The quality management system shall be assessed by the notified body, which shall determine whether it satisfies the requirements referred to in Article 17.

The decision shall be notified to the provider or its authorised representative.

The notification shall contain the conclusions of the assessment of the quality management system and the reasoned assessment decision.

3.3. The quality management system as approved shall continue to be implemented and maintained by the provider so that it remains adequate and efficient.

3.4. Any intended change to the approved quality management system or the list of AI systems covered by the latter shall be brought to the attention of the notified body by the provider.

The proposed changes shall be examined by the notified body, which shall decide whether the modified quality management system continues to satisfy the requirements referred to in point 3.2 or whether a reassessment is necessary.

The notified body shall notify the provider of its decision. The notification shall contain the conclusions of the examination of the changes and the reasoned assessment decision.

4. Control of the technical documentation.

4.1. In addition to the application referred to in point 3, an application with a notified body of their choice shall be lodged by the provider for the assessment of the technical documentation relating to the AI system which the provider intends to place on the market or put into service and which is covered by the quality management system referred to under point 3.

4.2. The application shall include:

(a) the name and address of the provider;

(b) a written declaration that the same application has not been lodged with any other notified body;

(c) the technical documentation referred to in Annex IV.

附件七

基于质量管理体系评估和评估的符合性

技术文档

1. 引言

基于质量管理体系评估和技术文档评估的合格评定是依据第2点至第5点的合格评定程序。

2. 概述

依据第17条批准的人工智能系统设计、开发和测试质量管理体系应依照第3点进行审查，并应接受第5点规定的监督。人工智能系统的技术文档应依照第4点进行审查。

3. 质量管理体系

3.1. 提供者的申请应包括：

(a) 提供者的名称和地址，以及如果申请由授权代表提出，该授权代表的名称和地址；

(b) 纳入同一质量管理体系的 AI 系统清单；

(c) 同一质量管理体系所涵盖的每个人工智能系统的技术文档；(d) 关于质量管理体系的文档，该文档应涵盖第17条所列的所有方面；

(e) 为确保质量管理体系保持充分和有效而制定的程序的说明；

(f) 一份书面声明，表明同一申请未提交给任何其他公告机构。

3.2. 质量管理体系应由公告机构进行评估，公告机构应确定其是否满足第17条所述的要求。

该决定应通知提供者或其授权代表。

通知应包含质量管理体系评估的结论和有理据的评估决定。

3.3. 经批准的质量管理体系应由提供者继续实施和维持，以使其保持充分和有效。

3.4. 对经批准的质量管理体系或其所涵盖的人工智能系统清单的任何预期变更，应由提供者提请公告机构注意。

拟议变更应由公告机构审查，该机构应决定修改后的质量管理体系是否继续满足第3.2点所述要求，或是否需要重新评估。

公告机构应将其决定通知提供者。通知应包含变更审查的结论和经论证的评估决定。

4. 技术文档的控制。

4.1. 除第3点所述的申请外，提供者还应向其选择的公告机构提交申请，以评估与提供者拟投放市场或投入使用且属于第3点所述质量管理体系涵盖范围的人工智能系统相关的技术文档。

4.2. 申请应包括：

(a) 提供者的名称和地址；

(b) 一份书面声明，表明同一申请未提交给任何其他公告机构；

(c) 附件IV所述技术文档。

4.3. The technical documentation shall be examined by the notified body. Where relevant, and limited to what is necessary to fulfil its tasks, the notified body shall be granted full access to the training, validation, and testing data sets used, including, where appropriate and subject to security safeguards, through API or other relevant technical means and tools enabling remote access.

4.4. In examining the technical documentation, the notified body may require that the provider supply further evidence or carry out further tests so as to enable a proper assessment of the conformity of the AI system with the requirements set out in Chapter III, Section 2. Where the notified body is not satisfied with the tests carried out by the provider, the notified body shall itself directly carry out adequate tests, as appropriate.

4.5. Where necessary to assess the conformity of the high-risk AI system with the requirements set out in Chapter III, Section 2, after all other reasonable means to verify conformity have been exhausted and have proven to be insufficient, and upon a reasoned request, the notified body shall also be granted access to the training and trained models of the AI system, including its relevant parameters. Such access shall be subject to existing Union law on the protection of intellectual property and trade secrets.

4.6. The decision of the notified body shall be notified to the provider or its authorised representative. The notification shall contain the conclusions of the assessment of the technical documentation and the reasoned assessment decision.

Where the AI system is in conformity with the requirements set out in Chapter III, Section 2, the notified body shall issue a Union technical documentation assessment certificate. The certificate shall indicate the name and address of the provider, the conclusions of the examination, the conditions (if any) for its validity and the data necessary for the identification of the AI system.

The certificate and its annexes shall contain all relevant information to allow the conformity of the AI system to be evaluated, and to allow for control of the AI system while in use, where applicable.

Where the AI system is not in conformity with the requirements set out in Chapter III, Section 2, the notified body shall refuse to issue a Union technical documentation assessment certificate and shall inform the applicant accordingly, giving detailed reasons for its refusal.

Where the AI system does not meet the requirement relating to the data used to train it, re-training of the AI system will be needed prior to the application for a new conformity assessment. In this case, the reasoned assessment decision of the notified body refusing to issue the Union technical documentation assessment certificate shall contain specific considerations on the quality data used to train the AI system, in particular on the reasons for non-compliance.

4.7. Any change to the AI system that could affect the compliance of the AI system with the requirements or its intended purpose shall be assessed by the notified body which issued the Union technical documentation assessment certificate. The provider shall inform such notified body of its intention to introduce any of the abovementioned changes, or if it otherwise becomes aware of the occurrence of such changes. The intended changes shall be assessed by the notified body, which shall decide whether those changes require a new conformity assessment in accordance with Article 43(4) or whether they could be addressed by means of a supplement to the Union technical documentation assessment certificate. In the latter case, the notified body shall assess the changes, notify the provider of its decision and, where the changes are approved, issue to the provider a supplement to the Union technical documentation assessment certificate.

5. Surveillance of the approved quality management system.

5.1. The purpose of the surveillance carried out by the notified body referred to in Point 3 is to make sure that the provider duly complies with the terms and conditions of the approved quality management system.

5.2. For assessment purposes, the provider shall allow the notified body to access the premises where the design, development, testing of the AI systems is taking place. The provider shall further share with the notified body all necessary information.

5.3. The notified body shall carry out periodic audits to make sure that the provider maintains and applies the quality management system and shall provide the provider with an audit report. In the context of those audits, the notified body may carry out additional tests of the AI systems for which a Union technical documentation assessment certificate was issued.

4.3. 技术文档应由公告机构审查。在相关情况下，且限于履行其任务所必需的范围，公告机构应被授予对所使用的训练、验证和测试数据集的完全访问权限，包括在适当情况下并在安全保障的前提下，通过API或其他能够实现远程访问的相关技术手段和工具进行访问。

4.4. 在审查技术文档时，公告机构可要求提供者提供进一步证据或进行进一步测试，以便对人工智能系统是否符合第三章第2节规定的要求进行适当评估。如果公告机构对提供者进行的测试不满意，公告机构应酌情自行直接进行适当的测试。

4.5. 在评估高风险人工智能系统是否符合Chapter III, Section 2中规定的要求有必要时，在已用尽所有其他合理手段验证符合性且证明这些手段不充分后，经说明理由的请求，公告机构还应被授予访问人工智能系统训练和已训练模型(包括其相关参数)的权限。此类访问应受现有关于知识产权和商业秘密保护的Union law约束。

4.6. 公告机构的决定应通知提供者或其授权代表。该通知应包含技术文档评估的结论和附有理由的评估决定。

人工智能系统符合Chapter III, Section 2中规定的要求时，公告机构应颁发欧盟技术文档评估证书。证书应载明提供者的名称和地址、审查结论、证书有效条件(如有)以及识别该人工智能系统所需的数据。

证书及其附件应包含所有相关信息，以便能够评估人工智能系统的符合性，并在适用情况下能够对使用中的人工智能系统进行控制。

当人工智能系统不符合第三章第2节规定的要求时，公告机构应拒绝签发欧盟技术文档评估证书，并相应通知申请人，说明拒绝的详细理由。

当人工智能系统不符合与其训练所用数据相关的要求时，在申请新的合格评定之前，将需要对人工智能系统进行重新训练。在此情况下，公告机构拒绝签发欧盟技术文档评估证书的附理由评估决定应包含关于用于训练人工智能系统的质量数据的具体考量，特别是关于不合规原因的考量。

4.7. 对人工智能系统的任何可能影响该系统符合要求或其预期目的的变更，应由签发Union technical documentation assessment certificate的公告机构进行评估。提供者应将其引入上述任何变更的意图告知该公告机构，或在其以其他方式知悉此类变更发生时告知。预期变更应由公告机构评估，该机构应决定这些变更是否需要根据Article 43(4)进行新的合格评定，或者是否可以通过对Union technical documentation assessment certificate的补充文件加以处理。在后一种情况下，公告机构应评估变更，将其决定通知提供者，并在变更获得批准时，向提供者签发Union technical documentation assessment certificate的补充文件。

5. 对已批准质量管理体系的监督。

5.1. 第3点所述公告机构进行的监督的目的是确保提供者适当遵守经批准的质量管理体系的条款和条件。

5.2. 为评估目的，提供者应允许公告机构进入进行人工智能系统设计、开发和测试的场所。提供者还应与公告机构共享所有必要信息。

5.3. 公告机构应进行定期审核，以确保提供者维持和适用质量管理体系，并应向提供者提供审核报告。在这些审核的背景下，公告机构可对已获得欧盟技术文档评估证书的人工智能系统进行额外测试。

ANNEX VIII

Information to be submitted upon the registration of high-risk AI systems in accordance with Article 49

Section A — Information to be submitted by providers of high-risk AI systems in accordance with Article 49(1)

The following information shall be provided and thereafter kept up to date with regard to high-risk AI systems to be registered in accordance with Article 49(1):

1. The name, address and contact details of the provider;
2. Where submission of information is carried out by another person on behalf of the provider, the name, address and contact details of that person;
3. The name, address and contact details of the authorised representative, where applicable;
4. The AI system trade name and any additional unambiguous reference allowing the identification and traceability of the AI system;
5. A description of the intended purpose of the AI system and of the components and functions supported through this AI system;
6. A basic and concise description of the information used by the system (data, inputs) and its operating logic;
7. The status of the AI system (on the market, or in service; no longer placed on the market/in service, recalled);
8. The type, number and expiry date of the certificate issued by the notified body and the name or identification number of that notified body, where applicable;
9. A scanned copy of the certificate referred to in point 8, where applicable;
10. Any Member States in which the AI system has been placed on the market, put into service or made available in the Union;
11. A copy of the EU declaration of conformity referred to in Article 47;
12. Electronic instructions for use; this information shall not be provided for high-risk AI systems in the areas of law enforcement or migration, asylum and border control management referred to in Annex III, points 1, 6 and 7;
13. A URL for additional information (optional).

Section B — Information to be submitted by providers of high-risk AI systems in accordance with Article 49(2)

The following information shall be provided and thereafter kept up to date with regard to AI systems to be registered in accordance with Article 49(2):

1. The name, address and contact details of the provider;
2. Where submission of information is carried out by another person on behalf of the provider, the name, address and contact details of that person;
3. The name, address and contact details of the authorised representative, where applicable;
4. The AI system trade name and any additional unambiguous reference allowing the identification and traceability of the AI system;
5. A description of the intended purpose of the AI system;
6. The condition or conditions under Article 6(3)based on which the AI system is considered to be not-high-risk;
7. A short summary of the grounds on which the AI system is considered to be not-high-risk in application of the procedure under Article 6(3);
8. The status of the AI system (on the market, or in service; no longer placed on the market/in service, recalled);
9. Any Member States in which the AI system has been placed on the market, put into service or made available in the Union.

附件八

根据注册高风险人工智能系统时需提交的信息

第49条

A部分 - 根据第49(1)条高风险人工智能系统提供者需提交的信息应提供以下信息，并此后针对根据第49(1)条注册的高风险人工智能系统保持更新：

1. 提供者的名称、地址和联系方式；
2. 如果信息由代表提供者的其他人提交，该人的名称、地址和联系方式；
3. 授权代表(如适用)的名称、地址和联系方式；
4. 人工智能系统的商品名称以及任何能够识别和追溯该人工智能系统的额外明确参考信息；
5. 人工智能系统预期用途的说明以及通过该人工智能系统支持的组件和功能的说明；
6. 系统所使用的信息(数据、输入)及其运行逻辑的基本简要说明；
7. 人工智能系统的状态(在市场上或在服务中；不再投放市场/不再在服务中；已召回)；
8. 公告机构签发的证书的类型、编号和到期日期，以及该公告机构的名称或识别号(如适用)；
9. 第8点所述证书的扫描件(如适用)；
10. 人工智能系统已在欧盟境内投放市场、投入使用或提供使用的任何成员国；
11. 第47条所指的欧盟符合性声明副本；
12. 电子使用说明；对于附件三第1、6和7点所述执法或移民、庇护和边境管制管理领域的高风险人工智能系统，不应提供此信息；
13. 用于附加信息的URL(可选)。

B部分 - 根据第49(2)条高风险人工智能系统提供者需提交的信息应提供以下信息，并此后针对根据第49(2)条注册的人工智能系统保持更新：

1. 提供者的名称、地址和联系方式；
2. 如果信息由代表提供者的其他人提交，该人的名称、地址和联系方式；
3. 授权代表(如适用)的名称、地址和联系方式；
4. 人工智能系统的商品名称以及任何能够识别和追溯该人工智能系统的额外明确参考信息；
5. 对AI系统预期用途的描述；
6. 根据第6(3)条将该人工智能系统视为非高风险的条件；
7. 适用第6(3)条程序将该人工智能系统视为非高风险的理由的简要概述；
8. 人工智能系统的状态(在市场上或在服务中；不再投放市场/不再在服务中；已召回)；
9. 人工智能系统已在欧盟境内投放市场、投入使用或提供使用的任何成员国。

Section C — Information to be submitted by deployers of high-risk AI systems in accordance with Article 49(3)

The following information shall be provided and thereafter kept up to date with regard to high-risk AI systems to be registered in accordance with Article 49(3):

1. The name, address and contact details of the deployer;
2. The name, address and contact details of the person submitting information on behalf of the deployer;
3. The URL of the entry of the AI system in the EU database by its provider;
4. A summary of the findings of the fundamental rights impact assessment conducted in accordance with Article 27;
5. A summary of the data protection impact assessment carried out in accordance with Article 35 of Regulation (EU) 2016/679 or Article 27 of Directive (EU) 2016/680 as specified in Article 26(8) of this Regulation, where applicable.

C部分 - 根据第49(3)条高风险人工智能系统部署者需提交的信息应提供以下信息，并此后针对根据第49(3)条注册的高风险人工智能系统保持更新：

1. 部署者的名称、地址和联系方式；
2. 代表部署者提交信息的人员的姓名、地址和联系方式；
3. 人工智能系统提供者在欧盟数据库中条目的URL;
4. 根据第27条进行的基本权利影响评估的结果摘要；
5. 根据(EU) 2016/679条例第35条或(EU) 2016/680指令第27条(如本条例第26(8)条所规定)进行的数据保护影响评估的摘要(如适用)。

ANNEX IX

Information to be submitted upon the registration of high-risk AI systems listed in Annex III in relation to testing in real world conditions in accordance with Article 60

The following information shall be provided and thereafter kept up to date with regard to testing in real world conditions to be registered in accordance with Article 60:

1. A Union-wide unique single identification number of the testing in real world conditions;
2. The name and contact details of the provider or prospective provider and of the deployers involved in the testing in real world conditions;
3. A brief description of the AI system, its intended purpose, and other information necessary for the identification of the system;
4. A summary of the main characteristics of the plan for testing in real world conditions;
5. Information on the suspension or termination of the testing in real world conditions.

附件九

附件三所列高风险人工智能系统注册时须提交的信息
关于根据第60条在真实世界条件下进行测试

对于将根据第60条注册的真实世界条件下测试，应提供以下信息，并此后保持更新：

1. 真实世界条件下测试的欧盟范围内唯一单一识别号；
2. 提供者或潜在提供者以及参与真实世界条件下测试的部署者的名称和联系方式；
3. 人工智能系统的简要说明、其预期目的以及识别该系统所需的其他信息；
4. 在真实世界条件下测试计划的主要特征摘要；
5. 关于暂停或终止在真实世界条件下测试的信息。

ANNEX X

Union legislative acts on large-scale IT systems in the area of Freedom, Security and Justice

1. Schengen Information System

(a) Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals (OJ L 312, 7.12.2018, p. 1).

(b) Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006 (OJ L 312, 7.12.2018, p. 14).

(c) Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU (OJ L 312, 7.12.2018, p. 56).

2. Visa Information System

(a) Regulation (EU) 2021/1133 of the European Parliament and of the Council of 7 July 2021 amending Regulations (EU) No 603/2013, (EU) 2016/794, (EU) 2018/1862, (EU) 2019/816 and (EU) 2019/818 as regards the establishment of the conditions for accessing other EU information systems for the purposes of the Visa Information System (OJ L 248, 13.7.2021, p. 1).

(b) Regulation (EU) 2021/1134 of the European Parliament and of the Council of 7 July 2021 amending Regulations (EC) No 767/2008, (EC) No 810/2009, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861, (EU) 2019/817 and (EU) 2019/1896 of the European Parliament and of the Council and repealing Council Decisions 2004/512/EC and 2008/633/JHA, for the purpose of reforming the Visa Information System (OJ L 248, 13.7.2021, p. 11).

3. Eurodac

Regulation (EU) 2024/1358 of the European Parliament and of the Council of 14 May 2024 on the establishment of 'Eurodac' for the comparison of biometric data in order to effectively apply Regulations (EU) 2024/1315 and (EU) 2024/1350 of the European Parliament and of the Council and Council Directive 2001/55/EC and to identify illegally staying third-country nationals and stateless persons and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, amending Regulations (EU) 2018/1240 and (EU) 2019/818 of the European Parliament and of the Council and repealing Regulation (EU) No 603/2013 of the European Parliament and of the Council (OJ L, 2024/1358, 22.5.2024, ELI: http://data.europa.eu/eli/reg/2024/1358/oj).

4. Entry/Exit System

Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011 (OJ L 327, 9.12.2017, p. 20).

5. European Travel Information and Authorisation System

(a) Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226 (OJ L 236, 19.9.2018, p. 1).

(b) Regulation (EU) 2018/1241 of the European Parliament and of the Council of 12 September 2018 amending Regulation (EU) 2016/794 for the purpose of establishing a European Travel Information and Authorisation System (ETIAS) (OJ L 236, 19.9.2018, p. 72).

附件十

自由、安全和司法领域大规模信息技术系统的欧盟立法法案

1. 申根信息系统

(a) 欧洲议会和理事会2018年11月28日关于利用申根信息系统遣返非法居留第三国国民的第(EU)2018/1860号条例(OJ L 312, 7.12.2018, p.1)。

(b) 欧洲议会和理事会2018年11月28日关于在边境检查领域建立、运行和使用申根信息系统(SIS)并修订执行《申根协定》的公约以及修订和废止第1987/2006号条例(EC)的第2018/1861号条例(EU)(OJ L 312,2018年12月7日，第14页)。

(c) 欧洲议会和理事会2018年11月28日关于在警务合作和刑事司法合作领域建立、运行和使用申根信息系统(SIS)的第(EU) 2018/1862号条例，修订并废止理事会第2007/533/JHA号决定，并废止欧洲议会和理事会第(EC) No 1986/2006号条例及委员会第2010/261/EU号决定(OJ L 312, 7.12.2018, p.56)。

2. 签证信息系统

(a) 欧洲议会和理事会2021年7月7日关于为签证信息系统目的确立访问其他欧盟信息系统条件的、修订第(EU) No 603/2013号、第(EU) 2016/794号、第(EU) 2018/1862号、第(EU) 2019/816号和第(EU) 2019/818号条例的第(EU) 2021/1133号条例(OJ L 248, 13.7.2021， 第1页)。

(b) 欧洲议会和理事会2021年7月7日为改革签证信息系统目的修订欧洲议会和理事会(EC) No 767/2008、(EC) No 810/2009、(EU) 2016/399、(EU) 2017/2226、(EU) 2018/1240、(EU) 2018/1860、(EU) 2018/1861、(EU) 2019/817和(EU) 2019/1896条例并废止理事会决定2004/512/EC和2008/633/JHA的(EU) 2021/1134条例(OJ L 248, 13.7.2021, p.11)。

3. 欧洲指纹

欧洲议会和欧盟理事会2024年5月14日关于建立"Eurodac"以比对生物特征数据，从而有效适用欧洲议会和欧盟理事会(EU) 2024/1315号条例和(EU) 2024/1350号条例及欧盟理事会2001/55/EC号指令，并识别非法居留的第三国国民和无国籍人士，以及关于成员国执法当局和欧洲刑警组织为执法目的请求与Eurodac数据进行比对的(EU) 2024/1358号条例，修订欧洲议会和欧盟理事会(EU) 2018/1240号条例和(EU) 2019/818号条例，并废止欧洲议会和欧盟理事会(EU) 第603/2013号条例(OJ L, 2024/1358, 22.5.2024, ELI: http://data.europa.eu/eli/reg/2024/1358/oj)。

4. 出入境系统

欧洲议会和理事会2017年11月30日第(EU) 2017/2226号条例，建立出入境系统(EES)，用于登记跨越成员国外部边界的第三国国民的出入境数据和拒绝入境数据，并确定出于执法目的访问EES的条件，并修订执行申根协定的公约以及第(EC) No 767/2008号和第(EU) No 1077/2011号条例(OJ L 327, 9.12.2017, p.20)。

5. 欧洲旅行信息与授权系统

(a) 欧洲议会和理事会2018年9月12日关于建立欧洲旅行信息和授权系统(ETIAS)并修订(EU) No 1077/2011、(EU) No 515/2014、(EU) 2016/399、(EU) 2016/1624和(EU) 2017/2226条例的(EU) 2018/1240条例(OJ L 236, 19.9.2018, p.1)。

(b) 欧洲议会和理事会2018年9月12日关于为建立欧洲旅行信息和授权系统(ETIAS)目的修订(EU) 2016/794条例的(EU) 2018/1241条例(OJ L 236, 19.9.2018, p.72)。

6. European Criminal Records Information System on third-country nationals and stateless persons

Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726 (OJ L 135, 22.5.2019, p. 1).

7. Interoperability

(a) Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA (OJ L 135, 22.5.2019, p. 27).

(b) Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816 (OJ L 135, 22.5.2019, p. 85).

6.第三国国民和无国籍人欧洲犯罪记录信息系统

欧洲议会和理事会2019年4月17日第(EU) 2019/816号条例，建立用于识别持有第三国国民和无国籍人定罪信息的成员国的集中化系统(ECRIS-TCN)，以补充欧洲犯罪记录信息系统，并修订第(EU) 2018/1726号条例(OJ L 135, 22.5.2019, p.1)。

7.互操作性

(a) 欧洲议会和理事会2019年5月20日关于在边境和签证领域建立欧盟信息系统间互操作性框架并修订欧洲议会和理事会(EC) No 767/2008、(EU) 2016/399、(EU) 2017/2226、(EU) 2018/1240、(EU) 2018/1726和(EU) 2018/1861条例及理事会决定2004/512/EC和2008/633/JHA的(EU) 2019/817条例(OJ L 135, 22.5.2019, p.27)。

(b) 欧洲议会和理事会2019年5月20日关于在警务和司法合作、庇护和移民领域建立欧盟信息系统间互操作性框架并修订(EU) 2018/1726、(EU) 2018/1862和(EU) 2019/816条例的(EU) 2019/818条例(OJ L 135, 22.5.2019, p.85)。

ANNEX XI

Technical documentation referred to in Article 53(1), point (a) — technical documentation for providers of general-purpose AI models

Section 1

Information to be provided by all providers of general-purpose AI models

The technical documentation referred to in Article 53(1), point (a) shall contain at least the following information as appropriate to the size and risk profile of the model:

1. A general description of the general-purpose AI model including:

   (a) the tasks that the model is intended to perform and the type and nature of AI systems in which it can be integrated;

   (b) the acceptable use policies applicable;

   (c) the date of release and methods of distribution;

   (d) the architecture and number of parameters;

   (e) the modality (e.g. text, image) and format of inputs and outputs;

   (f) the licence.

2. A detailed description of the elements of the model referred to in point 1, and relevant information of the process for the development, including the following elements:

   (a) the technical means (e.g. instructions of use, infrastructure, tools) required for the general-purpose AI model to be integrated in AI systems;

   (b) the design specifications of the model and training process, including training methodologies and techniques, the key design choices including the rationale and assumptions made; what the model is designed to optimise for and the relevance of the different parameters, as applicable;

   (c) information on the data used for training, testing and validation, where applicable, including the type and provenance of data and curation methodologies (e.g. cleaning, filtering, etc.), the number of data points, their scope and main characteristics; how the data was obtained and selected as well as all other measures to detect the unsuitability of data sources and methods to detect identifiable biases, where applicable;

   (d) the computational resources used to train the model (e.g. number of floating point operations), training time, and other relevant details related to the training;

   (e) known or estimated energy consumption of the model.

With regard to point (e), where the energy consumption of the model is unknown, the energy consumption may be based on information about computational resources used.

Section 2

Additional information to be provided by providers of general-purpose AI models with systemic risk

1. A detailed description of the evaluation strategies, including evaluation results, on the basis of available public evaluation protocols and tools or otherwise of other evaluation methodologies. Evaluation strategies shall include evaluation criteria, metrics and the methodology on the identification of limitations.

2. Where applicable, a detailed description of the measures put in place for the purpose of conducting internal and/or external adversarial testing (e.g. red teaming), model adaptations, including alignment and fine-tuning.

附件十一

第53(1)条第(a)点所述技术文档--的技术文档
通用人工智能模型提供者

第1节

通用人工智能模型的所有提供者应提供的信息

第53(1)条第(a)点所述技术文档应至少包含以下信息：
与模型的规模和风险状况相适应：

1. 通用人工智能模型的总体描述，包括：

   (a) 该模型预期执行的任务以及可集成该模型的人工智能系统的类型和性质；

   (b) 适用的可接受使用政策；

   (c) 发布日期和分发方法；

   (d) 架构和参数数量；

   (e) 输入和输出的模态(例如文本、图像)和格式；

   (f) 许可证。

2. 对第1点所述模型要素的详细说明，以及开发过程的相关信息，包括以下要素：

   (a) 通用人工智能模型集成到人工智能系统所需的技术手段(例如使用说明、基础设施、工具)；

   (b) 模型和训练过程的设计规格，包括训练方法和技术、关键设计选择(包括所作的理由和假设)；模型设计优化的目标以及不同参数的相关性(如适用)；

   (c) 关于用于训练、测试和验证的数据的信息(如适用)，包括数据的类型和来源以及整理方法(例如清洗、过滤等)、数据点数量、其范围和主要特征；数据如何获取和选择，以及为检测数据源不适用性而采取的所有其他措施和检测可识别偏见的方法(如适用)；

   (d) 用于训练模型的计算资源(例如浮点运算次数)、训练时间以及与训练相关的其他相关细节；

   (e) 模型的已知或估计能耗。

关于第(五)点，若模型的能耗未知，能耗可基于所用计算资源的信息进行估算。

第2节

具有系统性风险的通用人工智能模型提供者须提供的附加信息

1. 对评估策略的详细说明，包括基于现有公开评估协议和工具或其他评估方法的评估结果。评估策略应包括评估标准、指标以及识别局限性的方法。

2. 在适用情况下，详细说明为进行内部和/或外部对抗性测试(例如红队测试)、模型适配(包括对齐和微调)而采取的措施。

3. Where applicable, a detailed description of the system architecture explaining how software components build or feed into each other and integrate into the overall processing.

3. 在适用情况下，详细说明系统架构，解释软件组件如何相互构建或相互输入并集成到整体处理中。

ANNEX XII

Transparency information referred to in Article 53(1), point (b) — technical documentation for providers of general-purpose AI models to downstream providers that integrate the model into their AI system

The information referred to in Article 53(1), point (b) shall contain at least the following:

1. A general description of the general-purpose AI model including:
   (a) the tasks that the model is intended to perform and the type and nature of AI systems into which it can be integrated;
   (b) the acceptable use policies applicable;
   (c) the date of release and methods of distribution;
   (d) how the model interacts, or can be used to interact, with hardware or software that is not part of the model itself, where applicable;
   (e) the versions of relevant software related to the use of the general-purpose AI model, where applicable;
   (f) the architecture and number of parameters;
   (g) the modality (e.g. text, image) and format of inputs and outputs;
   (h) the licence for the model.
2. A description of the elements of the model and of the process for its development, including:
   (a) the technical means (e.g. instructions for use, infrastructure, tools) required for the general-purpose AI model to be integrated into AI systems;
   (b) the modality (e.g. text, image, etc.) and format of the inputs and outputs and their maximum size (e.g. context window length, etc.);
   (c) information on the data used for training, testing and validation, where applicable, including the type and provenance of data and curation methodologies.

附件十二

第53(1)条第(b)点所指的透明度信息--通用人工智能模型提供者向将该模型集成到其中的下游提供者提供的技术文档

人工智能系统

第53(1)条第(二)点所指的信息应至少包含以下内容：

1. 通用人工智能模型的总体描述，包括：
   (a) 模型预期执行的任务以及可集成该模型的人工智能系统的类型和性质；
   (b) 适用的可接受使用政策；
   (c) 发布日期和分发方法；
   (d) 在适用情况下，模型如何与不属于模型本身的硬件或软件交互，或可被用于与其交互；
   (e) 在适用情况下，与使用该通用人工智能模型相关的相关软件版本；
   (f) 架构和参数数量；(g) 输入和输出的模态(例如文本、图像)和格式；
   (h) 模型的许可证。
2. 对模型要素及其开发过程的描述，包括：
   (a) 通用人工智能模型集成到人工智能系统所需的技术手段(例如使用说明、基础设施、工具)；
   (b) 输入和输出的模态(例如文本、图像等)和格式及其最大规模(例如上下文窗口长度等)；
   (c) 在适用情况下，关于用于训练、测试和验证的数据的信息，包括数据的类型和来源以及数据整理方法。

ANNEX XIII

Criteria for the designation of general-purpose AI models with systemic risk referred to in Article 51

For the purpose of determining that a general-purpose AI model has capabilities or an impact equivalent to those set out in Article 51(1), point (a), the Commission shall take into account the following criteria:

(a) the number of parameters of the model;

(b) the quality or size of the data set, for example measured through tokens;

(c) the amount of computation used for training the model, measured in floating point operations or indicated by a combination of other variables such as estimated cost of training, estimated time required for the training, or estimated energy consumption for the training;

(d) the input and output modalities of the model, such as text to text (large language models), text to image, multi-modality, and the state of the art thresholds for determining high-impact capabilities for each modality, and the specific type of inputs and outputs (e.g. biological sequences);

(e) the benchmarks and evaluations of capabilities of the model, including considering the number of tasks without additional training, adaptability to learn new, distinct tasks, its level of autonomy and scalability, the tools it has access to;

(f) whether it has a high impact on the internal market due to its reach, which shall be presumed when it has been made available to at least 10 000 registered business users established in the Union;

(g) the number of registered end-users.

附件十三

第51条所指具有系统性风险的通用人工智能模型的指定标准

为确定通用人工智能模型具有与第51(1)条第(a)点所列能力或影响相当的能力或影响，委员会应考虑以下标准：(a) 模型的参数数量；(b) 数据集的质量或规模，例如通过token衡量；(c) 用于训练模型的计算量，以浮点运算衡量或由其他变量的组合表明，例如估计的训练成本、估计的训练所需时间或估计的训练能耗；

(d) 模型的输入和输出模态，例如文本到文本(大型语言模型)、文本到图像、多模态，以及用于确定每种模态高影响能力的最先进阈值，以及输入和输出的特定类型(例如生物序列)；

(e) 模型能力的基准测试和评估，包括考虑无需额外训练即可完成的任务数量、学习新的不同任务的适应性、其自主性和可扩展性水平、其可访问的工具；

(f) 其是否因其覆盖范围而对内部市场产生高影响，当其已提供给至少10 000名在联盟内设立的注册商业用户时，应推定具有此种高影响；

(g) 注册最终用户的数量。

How this file was made

This is a complete Chinese translation of the EU Artificial Intelligence Act (AI Act). Tables, captions, headers, footers and numbering all keep their original positions. Nothing has been cut.

If you have documents of your own

- Contracts, tenders, standards, patents, reports: original layout kept, CNY 0.15/page
- PDF to Word: free up to 100 pages, CNY 0.10/page beyond that
- Scanned or image-only PDFs: OCR to Word, free
- No sign-up, no login: upload and download

Open the address below and try it with your own file:

https://www.ivyivy.com.cn/eu-ai-act-2024-1689-zh

On-premise deployment available (subject to model and compliance review)

Machine translation, provided for reading reference only. For professional judgement and compliance citation, please refer to the original English source.

This page is a translator's note; it is not part of the original document.

这份文件是怎么做出来的

本译本是欧盟《人工智能法案（AI Act）》的中文全译本，共 144 页。表格、图注、页眉页脚、编号层级都按原文位置一一还原，未做任何删节。

你手上如果也有英文文件要处理

- 合同、标书、标准、专利、报告：翻译后保留原版式，0.15 元/页
- PDF 转 Word：100 页内免费，超出 0.1 元/页
- 扫描件、图片版 PDF：先 OCR 再转 Word，免费
- 不用注册、不用登录，传上去直接下载

打开下面这个地址，把你自己的文件传上去试试：

https://www.ivyivy.com.cn/eu-ai-act-2024-1689-zh

支持私有化部署（需按贵方模型与合规要求评估）

本译本由机器翻译生成，仅供阅读参考；专业技术判断与合规引用，请以英文原文为准。

本页为译制说明，不属于原文件内容。