2024/1689 12.7.2024

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

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) 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)。

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) 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

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

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) 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)。

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)。

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

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

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)。

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)。

(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）。

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

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

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

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)。

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。

(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) 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) 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) 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)。

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

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)。

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) 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)。

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

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

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

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)。

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) 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) 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) 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

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)。

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。

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) 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。

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，在这些系统用于执法、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)。

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，

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)。

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)。

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) 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. 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) “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) “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) ‘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) “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。

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) 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

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. 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. 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. 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. 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. 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。

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) 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) 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。

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) 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. 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。

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. 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。

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. 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。

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. 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. 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. 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。

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. 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. 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。

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) 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。

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. 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. 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. 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. 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. 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. 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.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.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) 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。

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) 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。

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. 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) 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) 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。

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) 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) 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) 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. 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) 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. 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. 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. 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) (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. 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. 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) 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)。

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. 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. 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。

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。

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. 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) 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。

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. 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. 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) 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) 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)。”。

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)。”。

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) 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)。

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. 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	提交理事会
主席	主席
R. 梅措拉	M. 米歇尔

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. 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。

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。

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) 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) 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。

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) 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。

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。

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。

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. 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。

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。

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)。

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。

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.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)。

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. 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。

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。

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。

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）

扫码关注服务号
咨询定制交付

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。