I

(Legislative acts)

REGULATIONS

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 27 April 2016

on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

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

Having regard to the proposal from the European Commission,

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

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

Having regard to the opinion of the Committee of the Regions ([2]),

Acting in accordance with the ordinary legislative procedure ([3]),

Whereas:

(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

(2) The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.

(3) Directive 95/46/EC of the European Parliament and of the Council ([4]) seeks to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to ensure the free flow of personal data between Member States.

([1]) OJ C 229, 31.7.2012, p. 90.
([2]) OJ C 391, 18.12.2012, p. 127.
([3]) Position of the European Parliament of 12 March 2014 (not yet published in the Official Journal) and position of the Council at first reading of 8 April 2016 (not yet published in the Official Journal). Position of the European Parliament of 14 April 2016.
([4]) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

I

(立法性法案)

条例

欧洲议会和理事会条例(EU)2016/679

2016年4月27日

关于在个人数据处理方面保护自然人以及关于此类数据自由流动，并废止 Directive 95/46/EC(通用数据保护条例)

(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，

考虑到欧洲联盟委员会提出的提案，

在将立法草案送交国家议会后，

考虑到欧洲经济和社会委员会的意见(1)，

考虑到区域委员会的意见(2)，

按照普通立法程序(3)行事，

鉴于：

(1) 在个人数据处理方面保护自然人是基本权利。《欧洲联盟基本权利宪章》("《宪章》")第8(1)条和《欧洲联盟运行条约》(TFEU)第16(1)条规定，人人有权保护与其相关的个人数据。

(2) 关于在个人数据处理方面保护自然人的原则和规则，无论其国籍或居所，均应尊重其基本权利和自由，特别是其个人数据受保护的权利。本条例旨在促进自由、安全和正义区域以及经济联盟的实现，促进经济和社会进步，加强和趋同内部市场内的经济体，并促进自然人的福祉。

(3) 欧洲议会和理事会指令95/46/EC(4)旨在协调在处理活动方面对自然人基本权利和自由的保护，并确保个人数据在成员国之间的自由流动。

(1) OJ C 229, 31.7.2012， 第90页。
(2) OJ C 391, 18.12.2012， 第127页。
(3) 欧洲议会2014年3月12日的立场(尚未在《官方公报》上公布)以及理事会2016年4月8日一读的立场(尚未在《官方公报》上公布)。欧洲议会2016年4月14日的立场。
(4) 欧洲议会和理事会1995年10月24日关于在个人数据处理方面保护个人以及此类数据自由流动的第95/46/EC号指令(OJ L 281, 23.11.1995,

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

(4) The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.

(5) The economic and social integration resulting from the functioning of the internal market has led to a substantial increase in cross-border flows of personal data. The exchange of personal data between public and private actors, including natural persons, associations and undertakings across the Union has increased. National authorities in the Member States are being called upon by Union law to cooperate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State.

(6) Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data.

(7) Those developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market. Natural persons should have control of their own personal data. Legal and practical certainty for natural persons, economic operators and public authorities should be enhanced.

(8) Where this Regulation provides for specifications or restrictions of its rules by Member State law, Member States may, as far as necessary for coherence and for making the national provisions comprehensible to the persons to whom they apply, incorporate elements of this Regulation into their national law.

(9) The objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the implementation of data protection across the Union, legal uncertainty or a widespread public perception that there are significant risks to the protection of natural persons, in particular with regard to online activity. Differences in the level of protection of the rights and freedoms of natural persons, in particular the right to the protection of personal data, with regard to the processing of personal data in the Member States may prevent the free flow of personal data throughout the Union. Those differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. Such a difference in levels of protection is due to the existence of differences in the implementation and application of Directive 95/46/EC.

(10) In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union. Regarding the processing of personal data for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Member States should be allowed to maintain or introduce national provisions to further specify the application of the rules of this Regulation. In conjunction with the general and horizontal law on data protection implementing Directive 95/46/EC, Member States have several sector-specific laws in areas that need more specific provisions. This Regulation also provides a margin of manoeuvre for Member States to specify its rules, including for the processing of special categories of personal data ('sensitive data'). To that extent, this Regulation does not exclude Member State law that sets out the circumstances for specific processing situations, including determining more precisely the conditions under which the processing of personal data is lawful.

(4) 个人数据的处理应旨在服务于人类。个人数据受保护的权利不是一项绝对权利；必须根据比例原则，考虑其在社会中的功能，并与其他基本权利相平衡。本条例尊重所有基本权利，并遵守《宪章》所承认的、载于各项条约的自由和原则，特别是对私人和家庭生活、住宅和通信的尊重，个人数据保护，思想、良心和宗教自由，表达和信息自由，经营自由，获得有效救济和公正审判的权利，以及文化、宗教和语言多样性。

(5) 内部市场运作所带来的经济和社会一体化导致个人数据跨境流动大幅增加。公共和私人行为者之间，包括整个欧盟范围内的自然人、协会和企业之间的个人数据交换有所增加。成员国国家当局被欧盟法要求开展合作并交换个人数据，以便能够履行职责或代表另一成员国当局执行任务。

(6) 快速的技术发展和全球化给个人数据保护带来了新的挑战。个人数据收集和共享的规模显著增加。技术使私营公司和公共当局能够以前所未有的规模利用个人数据来开展其活动。自然人越来越多地在全球范围内公开提供个人信息。技术改变了经济和社会生活，应进一步促进个人数据在欧盟内的自由流动以及向第三国和国际组织的转移，同时确保高水平的个人数据保护。

(7) 鉴于建立信任对于数字经济在整个内部市场发展的重要性，这些发展要求欧盟建立一个强大且更加一致的数据保护框架，并以强有力的执法为支撑。自然人应当能够控制自己的个人数据。应当增强自然人、经济运营者和公共当局在法律和实践上的确定性。

(8) 本条例由成员国法律对其规则作出具体规定或限制时，成员国可在为保持一致以及使国家规定对其适用对象易于理解所必需的范围内，将本条例的要素纳入其国家法律。

(9) 95/46/EC指令的目标和原则仍然合理，但该指令未能防止整个欧盟数据保护实施中的碎片化、法律不确定性或公众普遍认为自然人保护存在重大风险，特别是在线活动方面。成员国在个人数据处理方面对自然人权利和自由的保护水平，特别是个人数据受保护权利的差异，可能阻碍个人数据在整个欧盟的自由流动。因此，这些差异可能构成在欧盟层面开展经济活动的障碍，扭曲竞争，并妨碍当局履行欧盟法规定的职责。这种保护水平的差异是由于95/46/EC指令在实施和适用方面存在差异。

(10) 为确保对自然人提供一致且高水平的保护，并消除欧盟内部个人数据流动的障碍，各成员国对自然人有关此类数据处理的权利和自由的保护水平应当等同。应确保在整个欧盟范围内一致和统一地适用有关个人数据处理中保护自然人基本权利和自由的规则。关于为遵守法律义务、为执行公共利益任务或为行使赋予控制者的官方职权而进行的个人数据处理，应允许成员国维持或引入国家规定，以进一步明确本条例规则的适用。结合实施 Directive 95/46/EC 的通用和横向数据保护法律，成员国在需要更具体规定的领域还有若干部门特定法律。本条例还为成员国具体规定其规则留有回旋余地，包括针对特殊类别的个人数据(“敏感数据”)的处理。在此范围内，本条例不排除成员国法律规定特定处理情形的情形，包括更精确地确定个人数据处理合法性的条件。

(11) Effective protection of personal data throughout the Union requires the strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States.

(12) Article 16(2) TFEU mandates the European Parliament and the Council to lay down the rules relating to the protection of natural persons with regard to the processing of personal data and the rules relating to the free movement of personal data.

(13) In order to ensure a consistent level of protection for natural persons throughout the Union and to prevent divergences hampering the free movement of personal data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide natural persons in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective cooperation between the supervisory authorities of different Member States. The proper functioning of the internal market requires that the free movement of personal data within the Union is not restricted or prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data. To take account of the specific situation of micro, small and medium-sized enterprises, this Regulation includes a derogation for organisations with fewer than 250 employees with regard to record-keeping. In addition, the Union institutions and bodies, and Member States and their supervisory authorities, are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation. The notion of micro, small and medium-sized enterprises should draw from Article 2 of the Annex to Commission Recommendation 2003/361/EC ([1]).

(14) The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data. This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person.

(15) In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used. The protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system. Files or sets of files, as well as their cover pages, which are not structured according to specific criteria should not fall within the scope of this Regulation.

(16) This Regulation does not apply to issues of protection of fundamental rights and freedoms or the free flow of personal data related to activities which fall outside the scope of Union law, such as activities concerning national security. This Regulation does not apply to the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union.

(17) Regulation (EC) No 45/2001 of the European Parliament and of the Council ([2]) applies to the processing of personal data by the Union institutions, bodies, offices and agencies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data should be adapted to the principles and rules established in this Regulation and applied in the light of this Regulation. In order to provide a strong and coherent data protection framework in the Union, the necessary adaptations of Regulation (EC) No 45/2001 should follow after the adoption of this Regulation, in order to allow application at the same time as this Regulation.

(18) This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. Personal or

([1]) Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (C(2003) 1422) (OJ L 124, 20.5.2003, p. 36).

([2]) Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

(11) 在整个欧盟有效保护个人数据，要求加强并详细规定数据主体的权利以及处理和决定个人数据处理者的义务，还要求成员国在监督和确保遵守个人数据保护规则方面具有同等权力，并对侵权行为具有同等制裁。

(12) TFEU第16(2)条授权欧洲议会和理事会制定有关在个人数据处理方面保护自然人的规则以及有关个人数据自由流动的规则。

(13) 为确保在整个欧盟范围内对自然人提供一致的保护水平，并防止分歧妨碍个人数据在内部市场内的自由流动，有必要制定一项 Regulation，为经济运营者(包括微型、小型和中型企业)提供法律确定性和透明，并为所有成员国的自然人提供同等水平的可依法执行的权利以及控制者和处理者的义务和责任，以确保对个人数据处理进行一致监督，并在所有成员国实施同等制裁，以及不同成员国的监管机构之间开展有效合作。内部市场的正常运作要求，不得以与个人数据处理中保护自然人有关的理由限制或禁止个人数据在欧盟内的自由流动。考虑到微型、小型和中型企业的具体情况，本条例包含针对雇员少于 250 人的组织在记录保存方面的减损。此外，鼓励欧盟机构和机关以及成员国及其监管机构在适用本条例时考虑微型、小型和中型企业的具体需求。微型、小型和中型企业的概念应借鉴 Commission Recommendation 2003/361/EC(1) 附件第 2 条。

(14) 本条例所提供的保护应适用于自然人，无论其国籍或居住地，涉及其个人数据的处理。本条例不涵盖涉及法人的个人数据处理，特别是设立为法人的企业，包括法人的名称和形式以及法人的联系方式。

(15) 为防止造成严重的规避风险，对自然人的保护应在技术上中立，且不应取决于所使用的技术。对自然人的保护应适用于通过自动化方式进行的个人数据处理，以及人工处理，如果个人数据包含在或意图包含在档案系统中。未按照特定标准构建的文件或文件集及其封面页不应属于本条例的范围。

(16) 本条例不适用于与不属于欧盟法范围的活动相关的基本权利和自由的保护或个人数据自由流动问题，例如涉及国家安全的活动。本条例不适用于成员国在开展与欧盟共同外交和安全政策相关的活动时对个人数据的处理。

(17) Regulation(EC) No 45/2001 of the European Parliament and of the Council(2) 适用于欧盟机构、机关、办事处和机构对个人数据的处理。Regulation(EC) No 45/2001 以及适用于此类个人数据处理的其他欧盟法律行为，应依照本条例确立的原则和规则进行调整，并依本条例予以适用。为在欧盟提供强有力且一致的数据保护框架，对 Regulation(EC) No 45/2001 的必要调整应在本条例通过后进行，以便与本条例同时适用。

(18) 本条例不适用于自然人在纯粹个人或家庭活动过程中对个人数据的处理，因而与专业或商业活动无关。个人或

(1) 委员会2003年5月6日关于微型、小型和中型企业定义的建议(C(2003) 1422)(OJ L 124,2003年5月20日，第36页)。

(2) 欧洲议会和理事会2000年12月18日关于在共同体机构和机关处理个人数据方面保护个人以及此类数据自由流动的第45/2001号条例(EC) (OJ L 8,2001年1月12日，第1页)。

household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities.

(19) The protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and the free movement of such data, is the subject of a specific Union legal act. This Regulation should not, therefore, apply to processing activities for those purposes. However, personal data processed by public authorities under this Regulation should, when used for those purposes, be governed by a more specific Union legal act, namely Directive (EU) 2016/680 of the European Parliament and of the Council ([1]). Member States may entrust competent authorities within the meaning of Directive (EU) 2016/680 with tasks which are not necessarily carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and prevention of threats to public security, so that the processing of personal data for those other purposes, in so far as it is within the scope of Union law, falls within the scope of this Regulation.

With regard to the processing of personal data by those competent authorities for purposes falling within scope of this Regulation, Member States should be able to maintain or introduce more specific provisions to adapt the application of the rules of this Regulation. Such provisions may determine more precisely specific requirements for the processing of personal data by those competent authorities for those other purposes, taking into account the constitutional, organisational and administrative structure of the respective Member State. When the processing of personal data by private bodies falls within the scope of this Regulation, this Regulation should provide for the possibility for Member States under specific conditions to restrict by law certain obligations and rights when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific important interests including public security and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. This is relevant for instance in the framework of anti-money laundering or the activities of forensic laboratories.

(20) While this Regulation applies, inter alia, to the activities of courts and other judicial authorities, Union or Member State law could specify the processing operations and processing procedures in relation to the processing of personal data by courts and other judicial authorities. The competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of the judiciary in the performance of its judicial tasks, including decision-making. It should be possible to entrust supervision of such data processing operations to specific bodies within the judicial system of the Member State, which should, in particular ensure compliance with the rules of this Regulation, enhance awareness among members of the judiciary of their obligations under this Regulation and handle complaints in relation to such data processing operations.

(21) This Regulation is without prejudice to the application of Directive 2000/31/EC of the European Parliament and of the Council ([2]), in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive. That Directive seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between Member States.

(22) Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.

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

([2]) Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ L 178, 17.7.2000, p. 1).

家庭活动可包括通信和保存地址，或在此类活动背景下进行的社交网络和在线活动。但是，本条例适用于为此类个人或家庭活动提供个人数据处理手段的控制者或处理者。

(19) 主管机构为预防、调查、侦查或起诉刑事犯罪或执行刑事处罚之目的处理个人数据时对自然人的保护，包括防范和预防对公共安全的威胁以及此类数据的自由流动，是特定欧盟法律行为的主题。因此，本条例不应适用于为这些目的的处理活动。然而，公共机构根据本条例处理的个人数据，在用于这些目的时，应受更具体的欧盟法律行为管辖，即Directive(EU) 2016/680 of the European Parliament and of the Council(1)。成员国可委托 Directive(EU) 2016/680 含义内的主管机构执行不一定为预防、调查、侦查或起诉刑事犯罪或执行刑事处罚之目的而执行的任务，包括防范和预防对公共安全的威胁，以便为这些其他目的进行的个人数据处理，只要属于欧盟法范围，即属于本条例的范围。

对于主管机关为本条例范围内目的处理个人数据，成员国应能够维持或引入更具体的规定，以调整本条例规则的适用。此类规定可更精确地确定主管机关为其他目的处理个人数据的具体要求，同时考虑各成员国的宪法、组织和行政结构。当私人机构处理个人数据属于本条例范围时，本条例应规定成员国在特定条件下可通过法律限制某些义务和权利的可能性，前提是此类限制构成民主社会中为保障特定重要利益(包括公共安全以及预防、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)所必需且相称的措施。例如，这在反洗钱框架或法医实验室活动中具有相关性。

(20) 尽管本条例适用于法院和其他司法机构的活动等，但联盟或成员国法律可规定法院和其他司法机构处理个人数据的处理操作和处理程序。当法院以其司法身份行事时，监管机构的职权不应涵盖个人数据处理，以保障司法机构在履行其司法任务(包括决策)时的独立性。应有可能将此类数据处理操作的监督委托给成员国司法系统内的特定机构，这些机构应特别确保遵守本条例规则，提高司法机构成员对本条例义务的认识，并处理与此类数据处理操作相关的投诉。

(21) 本条例不影响欧洲议会和理事会指令2000/31/EC(2)的适用，特别是该指令第12至15条中关于中介服务提供者责任规则的规定。该指令旨在通过确保信息社会服务在成员国之间的自由流动，促进内部市场的正常运作。

(22) 控制者或处理者在联盟内设立机构的活动背景下的任何个人数据处理，均应依照本条例进行，无论处理本身是否在联盟内进行。设立意味着通过稳定安排有效和真实地开展活动。此类安排的法律形式，无论是通过分支机构还是具有法律人格的子公司，在这方面不是决定性因素。

(1) 欧洲议会和欧盟理事会2016年4月27日关于主管机关为预防、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的第(EU) 2016/680号指令，并废除理事会第2008/977/JHA号框架决定(见本官方公报第89页)。

(2) 欧洲议会和理事会2000年6月8日关于信息社会服务特别是内部市场电子交易若干法律方面的指令2000/31/EC("电子交易指令")(OJ L 178, 17.7.2000, p.1)。

(23) In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment. In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union. Whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.

(24) The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union. In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.

(25) Where Member State law applies by virtue of public international law, this Regulation should also apply to a controller not established in the Union, such as in a Member State's diplomatic mission or consular post.

(26) The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

(27) This Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons.

(28) The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations. The explicit introduction of 'pseudonymisation' in this Regulation is not intended to preclude any other measures of data protection.

(29) In order to create incentives to apply pseudonymisation when processing personal data, measures of pseudonymisation should, whilst allowing general analysis, be possible within the same controller when that controller has taken technical and organisational measures necessary to ensure, for the processing concerned, that this Regulation is implemented, and that additional information for attributing the personal data to a specific data subject is kept separately. The controller processing the personal data should indicate the authorised persons within the same controller.

(23) 为确保自然人不会被剥夺本条例赋予其的保护，未在联盟设立的控制者或处理者对在联盟内的数据主体的个人数据处理，在处理活动涉及向此类数据主体提供商品或服务时(无论是否与付款相关)，应受本条例约束。为确定此类控制者或处理者是否向在联盟内的数据主体提供商品或服务，应查明控制者或处理者是否明显设想向联盟内一个或多个成员国的数据主体提供服务。仅控制者、处理者或中介的网站在联盟内可访问、电子邮件地址或其他联系方式可获取，或使用控制者设立地第三国通常使用的语言，不足以查明此类意图；使用一个或多个成员国通常使用的语言或货币并可用该另一语言订购商品和服务，或提及在联盟内的客户或用户等因素，可表明控制者设想向联盟内的数据主体提供商品或服务。

(24) 未在联盟设立的控制者或处理者对在联盟内的数据主体的个人数据处理，在涉及对此类数据主体行为的监控且其行为发生在联盟内时，也应受本条例约束。为确定某项处理活动是否可被视为监控数据主体的行为，应查明自然人在互联网上是否被追踪，包括可能后续使用个人数据处理技术进行画像，特别是为了对其作出决定或分析或预测其个人偏好、行为和态度。

(25) 成员国法律因国际公法而适用时，本条例也应适用于未在欧盟设立的控制者，例如在成员国的外交使团或领事馆。

(26) 数据保护原则应适用于任何与已识别或可识别的自然人有关的任何信息。经过假名化处理、但可通过使用额外信息归属于某一自然人的个人数据，应被视为可识别自然人的信息。为确定某一自然人是否可识别，应考虑控制者或另一人直接或间接识别该自然人所合理可能使用的一切手段，例如单独识别。为确定识别该自然人的手段是否合理可能被使用，应考虑一切客观因素，例如识别的成本和所需时间，并顾及处理时可得的技术和技术发展。因此，数据保护原则不应适用于匿名信息，即与已识别或可识别的自然人无关的信息，或经匿名化处理致使数据主体无法或不再可识别的个人数据。因此，本条例不涉及对此类匿名信息的处理，包括为统计或研究目的的处理。

(27) 本条例不适用于已故者的个人数据。成员国可规定关于已故者个人数据处理的规则。

(28) 对个人数据适用假名化可以降低相关数据主体的风险，并帮助控制者和处理者履行其数据保护义务。本条例明确引入"假名化"并非旨在排除任何其他数据保护措施。

(29) 为在处理个人数据时创造适用假名化的激励，在同一控制者已采取必要的技术和组织措施以确保就相关处理实施本条例、并将用于将个人数据归属于特定数据主体的额外信息单独保存的情况下，应允许该控制者内部采取假名化措施，同时允许进行一般分析。处理个人数据的控制者应指明同一控制者内部的授权人员。

(30) Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.

(31) Public authorities to which personal data are disclosed in accordance with a legal obligation for the exercise of their official mission, such as tax and customs authorities, financial investigation units, independent administrative authorities, or financial market authorities responsible for the regulation and supervision of securities markets should not be regarded as recipients if they receive personal data which are necessary to carry out a particular inquiry in the general interest, in accordance with Union or Member State law. The requests for disclosure sent by the public authorities should always be in writing, reasoned and occasional and should not concern the entirety of a filing system or lead to the interconnection of filing systems. The processing of personal data by those public authorities should comply with the applicable data-protection rules according to the purposes of the processing.

(32) Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

(33) It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.

(34) Genetic data should be defined as personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained.

(35) Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council ([1]) to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.

(36) The main establishment of a controller in the Union should be the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union, in which case that other establishment should be considered to be

([1]) Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45).

(30) 自然人可能与其设备、应用程序、工具和协议提供的在线标识符相关联，例如互联网协议地址、cookie标识符或其他标识符，如射频识别标签。这可能留下痕迹，特别是与唯一标识符和服务器接收的其他信息结合时，可用于创建自然人的画像并识别他们。

(31) 依照法律义务为履行其公务而向其披露个人数据的公共机关，例如税务和海关机关、金融调查单位、独立行政机关或负责证券市场监管和 supervision 的金融市场主管机关，如依照 Union 或 Member State 法律收到为公共利益开展特定调查所必需的个人数据，不应被视为接收方。公共机关发出的披露请求应始终以书面形式提出、说明理由且为偶发性，不应涉及整个档案系统或导致档案系统的互联。这些公共机关对个人数据的处理应依照处理目的遵守适用的数据保护规则。

(32) 同意应通过明确肯定的行为作出，以表明数据主体自由作出、具体、知情且明确无误地同意处理与其有关的个人数据，例如通过书面声明(包括电子方式)或口头声明。这可以包括在访问互联网网站时勾选方框、为信息社会服务选择技术设置，或在相关情境下明确表明数据主体接受对其个人数据拟议处理的其他声明或行为。因此，沉默、预先勾选的方框或不作为不应构成同意。同意应涵盖为同一目的或若干目的进行的所有处理活动。当处理具有多重目的时，应就所有目的取得同意。如数据主体的同意是在通过电子方式提出请求后作出，该请求必须清晰、简洁且不对所提供服务的使用造成不必要的干扰。

(33) 在数据收集时，通常无法完全确定出于科学研究目的处理个人数据的目的。因此，在符合公认的科学研究伦理标准的情况下，应允许数据主体对某些科学研究领域给予同意。在预期目的允许的范围内，数据主体应有机会仅对某些研究领域或研究项目的部分内容给予同意。

(34) 基因数据应定义为与自然人遗传或获得的遗传特征相关的个人数据，这些特征来自对有关自然人生物样本的分析，特别是染色体、脱氧核糖核酸(DNA)或核糖核酸(RNA)分析，或来自对能够获得同等信息的另一要素的分析。

(35) 与健康有关的个人数据应包括与数据主体健康状况有关的所有数据，这些数据揭示与数据主体过去、当前或未来的身体或精神健康状况有关的信息。这包括在向自然人注册或提供欧洲议会和理事会指令 2011/24/EU(1) 所指的医疗保健服务过程中收集的关于该自然人的信息；为健康目的分配给自然人以唯一识别该自然人的编号、符号或特定标识；从对身体部位或身体物质的检测或检查中获得的信息，包括从遗传数据和生物样本中获得的信息；以及关于例如疾病、残疾、疾病风险、病史、临床治疗或数据主体生理或生物医学状态的任何信息，无论其来源如何，例如来自医生或其他卫生专业人员、医院、医疗器械或体外诊断检测的信息。

(36) 控制者在欧盟的主要设立地应为其在欧盟的中央管理机构所在地，除非关于个人数据处理目的和手段的决定是在控制者在欧盟的另一设立地作出的，在此情况下，该另一设立地应被视为

(1) 欧洲议会和理事会2011年3月9日关于跨境医疗保健中患者权利适用的指令2011/24/EU(OJ L 88, 4.4.2011, p.45)。

the main establishment. The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes and means of processing through stable arrangements. That criterion should not depend on whether the processing of personal data is carried out at that location. The presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute a main establishment and are therefore not determining criteria for a main establishment. The main establishment of the processor should be the place of its central administration in the Union or, if it has no central administration in the Union, the place where the main processing activities take place in the Union. In cases involving both the controller and the processor, the competent lead supervisory authority should remain the supervisory authority of the Member State where the controller has its main establishment, but the supervisory authority of the processor should be considered to be a supervisory authority concerned and that supervisory authority should participate in the cooperation procedure provided for by this Regulation. In any case, the supervisory authorities of the Member State or Member States where the processor has one or more establishments should not be considered to be supervisory authorities concerned where the draft decision concerns only the controller. Where the processing is carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered to be the main establishment of the group of undertakings, except where the purposes and means of processing are determined by another undertaking.

(37) A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exert a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented. An undertaking which controls the processing of personal data in undertakings affiliated to it should be regarded, together with those undertakings, as a group of undertakings.

(38) Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.

(39) Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing.

(40) In order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or

主要营业机构。控制者在欧盟的主要营业机构应根据客观标准确定，并应意味着通过稳定的安排有效和真实地行使确定有关处理目的和方式的主要决策的管理活动。该标准不应取决于个人数据的处理是否在该地点进行。用于处理个人数据的技术手段和技术的存在和使用本身并不构成主要营业机构，因此不是主要营业机构的决定标准。处理者的主要营业机构应是其在欧盟的中央管理机构所在地，或者，如果其在欧盟没有中央管理机构，则是其在欧盟进行主要处理活动的地点。在同时涉及控制者和处理者的情况下，主管主导监管机构应仍为控制者主要营业机构所在成员国的监管机构，但处理者的监管机构应被视为有关监管机构，该监管机构应参与本条例规定的合作程序。在任何情况下，如果决定草案仅涉及控制者，则处理者在一个或多个成员国设有一个或多个营业机构的该成员国的监管机构不应被视为有关监管机构。如果处理由企业集团进行，则控制性企业的主要营业机构应被视为该企业集团的主要营业机构，除非处理的目的和方式由另一企业确定。

(37) 企业集团应涵盖控制性企业及其受控企业，其中控制性企业应是能够凭借例如所有权、财务参与或管辖其的规则或实施个人数据保护规则的权力而对其他企业施加主导影响的企业。控制其附属企业中个人数据处理的企业应与这些企业一起被视为企业集团。

(38) 儿童在其个人数据方面值得特殊保护，因为他们可能较少意识到有关风险、后果和保障措施以及他们与个人数据处理相关的权利。这种特殊保护尤其应适用于为营销或创建人格或用户画像目的使用儿童的个人数据，以及在使用直接向儿童提供的服务时收集儿童的个人数据。在直接向儿童提供的预防或咨询服务中，不应需要父母责任持有人的同意。

(39) 任何个人数据的处理都应合法和公平。应向自然人透明地说明有关其个人数据被收集、使用、查阅或以其他方式处理，以及个人数据正在或将要被处理的程度。透明原则要求与这些个人数据处理有关的任何信息和通信都应易于获取和易于理解，并使用清晰平实的语言。该原则尤其涉及向数据主体提供的关于控制者身份和处理目的的信息，以及确保对有关自然人进行公平和透明处理及其获得关于正在处理的有关其个人数据的确认和通信的权利的进一步信息。应使自然人了解与个人数据处理有关的风险、规则、保障措施和权利，以及如何行使与这种处理有关的权利。特别是，处理个人数据的具体目的应是明确和合法的，并在收集个人数据时确定。个人数据应充分、相关并限于处理目的所必需的范围。这尤其要求确保个人数据的存储期限限于严格的最低限度。只有在处理目的无法通过其他方式合理实现时，才应处理个人数据。为确保个人数据不被保存超过必要期限，控制者应设定删除或定期审查的时限。应采取一切合理步骤确保不准确的个人数据得到更正或删除。应以确保个人数据适当安全和保密的方式处理个人数据，包括防止未经授权访问或使用个人数据和用于处理的设备。

(40) 为使处理合法，个人数据应基于有关数据主体的同意或法律规定的某些其他合法依据进行处理，无论是本条例还是其他欧盟或

Member State law as referred to in this Regulation, including the necessity for compliance with the legal obligation to which the controller is subject or the necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

(41) Where this Regulation refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned. However, such a legal basis or legislative measure should be clear and precise and its application should be foreseeable to persons subject to it, in accordance with the case-law of the Court of Justice of the European Union (the 'Court of Justice') and the European Court of Human Rights.

(42) Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. In accordance with Council Directive 93/13/EEC ([1]) a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

(43) In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.

(44) Processing should be lawful where it is necessary in the context of a contract or the intention to enter into a contract.

(45) Where processing is carried out in accordance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, the processing should have a basis in Union or Member State law. This Regulation does not require a specific law for each individual processing. A law as a basis for several processing operations based on a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority may be sufficient. It should also be for Union or Member State law to determine the purpose of processing. Furthermore, that law could specify the general conditions of this Regulation governing the lawfulness of personal data processing, establish specifications for determining the controller, the type of personal data which are subject to the processing, the data subjects concerned, the entities to which the personal data may be disclosed, the purpose limitations, the storage period and other measures to ensure lawful and fair processing. It should also be for Union or Member State law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or, where it is in the public interest to do so, including for health purposes such as public health and social protection and the management of health care services, by private law, such as a professional association.

(46) The processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data

([1]) Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (OJ L 95, 21.4.1993, p. 29).

本条例所指的成员国法律，包括为遵守控制者所承担的法律义务所必需，或为履行数据主体作为一方的合同所必需，或应数据主体在订立合同前的要求采取措施所必需。

(41) 当本条例提及法律依据或立法措施时，这并不必然要求由议会通过立法法案，但不影响根据相关成员国宪法秩序的要求。然而，此类法律依据或立法措施应当明确和精确，且其适用应当对受其约束的人可预见，符合欧盟法院("法院")和欧洲人权法院的判例法。

(42) 当处理基于数据主体的同意时，控制者应当能够证明数据主体已同意该处理操作。特别是在关于另一事项的书面声明的背景下，保障措施应当确保数据主体知悉同意的事实及同意的范围。根据理事会指令93/13/EEC(1)，由控制者预先制定的同意声明应当以可理解和易于获取的形式提供，使用清晰和简明的语言，且不应包含不公平条款。为使同意为知情同意，数据主体至少应当知悉控制者的身份以及个人数据所意图用于的处理目的。如果数据主体没有真正或自由的选择，或无法在不遭受不利影响的情况下拒绝或撤回同意，则同意不应被视为自由给予。

(43) 为确保同意是自由给予的，在特定情况下，如果数据主体与控制者之间存在明显不平衡，特别是当控制者是公共机构且因此在特定情况的所有情形下同意不太可能是自由给予的，则同意不应为个人数据处理提供有效法律依据。如果同意不允许对不同个人数据处理操作分别给予同意，尽管在个别情况下这是适当的，或者如果合同的履行(包括提供某项服务)依赖于同意，而此类同意对于该履行并非必要，则推定同意不是自由给予的。

(44) 在合同背景下或有意订立合同时所必需的处理应属合法。

(45) 当处理是根据控制者所承担的法律义务进行的，或者当处理是为执行公共利益任务或行使官方权力所必需时，该处理应当有欧盟或成员国法律作为依据。本条例不要求每项单独处理都有特定法律。作为基于控制者所承担的法律义务或处理是为执行公共利益任务或行使官方权力所必需的多项处理操作的依据，一部法律可能就足够了。处理目的也应当由欧盟或成员国法律规定。此外，该法律可以规定本条例中管辖个人数据处理合法性的通用条件，确立用于确定控制者、受处理约束的个人数据类别、相关数据主体、个人数据可被披露给的实体、目的限制、存储期限以及确保合法和公平处理的其他措施的规范。控制者执行公共利益任务或行使官方权力时应当是公共机构或受公法管辖的另一自然人或法人，还是在公共利益要求如此时(包括出于公共卫生和社会保护以及医疗保健服务管理等健康目的)由私法管辖，例如专业协会，也应当由欧盟或成员国法律规定。

(46) 为保护数据主体或另一自然人的生命所必需的利益时，个人数据的处理也应被视为合法。个人数据的处理

(1) 1993年4月5日关于消费者合同中不公平条款的理事会指令93/13/EEC(OJ L 95, 21.4.1993, p.29)。

based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters.

(47) The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing. Given that it is for the legislator to provide by law for the legal basis for public authorities to process personal data, that legal basis should not apply to the processing by public authorities in the performance of their tasks. The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.

(48) Controllers that are part of a group of undertakings or institutions affiliated to a central body may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data. The general principles for the transfer of personal data, within a group of undertakings, to an undertaking located in a third country remain unaffected.

(49) The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.

(50) The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required. If the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Union or Member State law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. The legal basis provided by Union or Member State law for the processing of personal data may also provide a legal basis for further processing. In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, inter alia: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their

基于另一自然人的重大利益的处理，原则上仅应在处理不能明显基于另一法律依据时进行。某些类型的处理可能同时服务于重要的公共利益理由和数据主体的重大利益，例如当处理为人道主义目的所必需时，包括监测流行病及其传播或在人道主义紧急情况下，特别是自然和人为灾害情况下。

(47) 控制者的正当利益，包括个人数据可能被披露给的控制者的正当利益，或第三方的正当利益，可以为处理提供法律依据，前提是数据主体的利益或基本权利和自由不优先于该等利益，同时应考虑数据主体基于其与控制者之间关系的合理预期。例如，在数据主体是控制者的客户或服务于控制者的情形下，数据主体与控制者之间存在相关且适当的关系，此种正当利益即可存在。无论如何，正当利益的存在需要仔细评估，包括评估数据主体在个人数据收集之时和情境下能否合理预期为该目的进行的处理。在数据主体不能合理预期进一步处理的情形下处理个人数据时，数据主体的利益和基本权利尤其可能优先于数据控制者的利益。鉴于应由立法者为公共机关处理个人数据提供法律依据，该法律依据不应适用于公共机关履行其任务时的处理。为防止欺诈所严格必需的个人数据处理，也构成相关数据控制者的正当利益。为直接营销目的处理个人数据可被视为是为正当利益而进行的。

(48) 属于企业集团或隶属于中心机构的机构的控制者，为内部管理目的(包括处理客户或员工的个人数据)在企业集团内传输个人数据，可能具有正当利益。企业集团内向位于第三国的企业传输个人数据的一般原则不受影响。

(49) 在为确保网络和信息安全所严格必需且相称的范围内处理个人数据，即网络或信息系统在给定置信水平下抵御损害存储或传输的个人数据的可用性、真实性、完整性和保密性以及这些网络和系统所提供或可经由其访问的相关服务的安全的意外事件或非法或恶意行为的能力，由公共机关、计算机应急响应小组(CERTs)、计算机安全事件响应小组(CSIRTs)、电子通信网络和服务提供商以及安全技术和服务提供商进行的此类处理，构成相关数据控制者的正当利益。例如，这可包括防止未经授权访问电子通信网络和恶意代码传播，以及阻止"拒绝服务"攻击和对计算机及电子通信系统的损害。

(50) 仅为个人数据最初收集目的之外的其他目的处理个人数据，应仅在该处理与最初收集个人数据的目的相兼容时才被允许。在此种情况下，无需在允许收集个人数据的法律依据之外另行具备法律依据。如果处理是为履行公共利益任务或行使赋予控制者的官方职权所必需，Union或成员国法律可确定并规定进一步处理应被视为相兼容且合法的任务和目的。为公共利益存档目的、科学或历史研究目的或统计目的进行的进一步处理，应被视为相兼容的合法处理操作。Union或成员国法律为个人数据处理提供的法律依据，也可为进一步处理提供法律依据。为确定进一步处理的目的是否与最初收集个人数据的目的相兼容，控制者在满足原始处理合法性的所有要求后，应尤其考虑：这些目的与拟进一步处理目的之间的任何联系；个人数据被收集的情境，特别是数据主体基于其与控制者的关系对其

further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations.

进一步使用；个人数据的性质；预期进一步处理对数据主体的后果；以及原始处理和预期进一步处理操作中是否存在适当保障措施。

Where the data subject has given consent or the processing is based on Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard, in particular, important objectives of general public interest, the controller should be allowed to further process the personal data irrespective of the compatibility of the purposes. In any case, the application of the principles set out in this Regulation and in particular the information of the data subject on those other purposes and on his or her rights including the right to object, should be ensured. Indicating possible criminal acts or threats to public security by the controller and transmitting the relevant personal data in individual cases or in several cases relating to the same criminal act or threats to public security to a competent authority should be regarded as being in the legitimate interest pursued by the controller. However, such transmission in the legitimate interest of the controller or further processing of personal data should be prohibited if the processing is not compatible with a legal, professional or other binding obligation of secrecy.

如果数据主体已给予同意，或处理基于Union或成员国法律，且该法律构成民主社会中为保障特别是重大公共利益目标所必需且相称的措施，则应允许控制者进一步处理个人数据，而不论目的是否相兼容。在任何情况下，均应确保适用本条例规定的原则，特别是确保数据主体知悉该等其他目的及其权利，包括反对权。控制者表明可能存在犯罪行为或对公共安全的威胁，并在个案中或在与同一犯罪行为或对公共安全的威胁相关的若干案件中向主管机关传输相关个人数据，应被视为属于控制者所追求的正当利益。但是，如果处理与控制者合法的、职业的或其他有约束力的保密义务不相兼容，则应禁止为控制者的正当利益进行此类传输或进一步处理个人数据。

(51) Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data should include personal data revealing racial or ethnic origin, whereby the use of the term 'racial origin' in this Regulation does not imply an acceptance by the Union of theories which attempt to determine the existence of separate human races. The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person. Such personal data should not be processed, unless processing is allowed in specific cases set out in this Regulation, taking into account that Member States law may lay down specific provisions on data protection in order to adapt the application of the rules of this Regulation for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. In addition to the specific requirements for such processing, the general principles and other rules of this Regulation should apply, in particular as regards the conditions for lawful processing. Derogations from the general prohibition for processing such special categories of personal data should be explicitly provided, inter alia, where the data subject gives his or her explicit consent or in respect of specific needs in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.

(51) 就其性质而言与基本权利和自由相关的特别敏感的个人数据值得特别保护，因为其处理情境可能对基本权利和自由造成重大风险。该等个人数据应包括揭示种族或民族出身、政治观点、宗教或哲学信仰或工会成员身份的个人数据，以及基因数据、为唯一识别自然人而处理生物特征数据、健康数据或有关自然人性生活或性取向的数据。此类个人数据不应被处理，除非本条例规定的特定情形允许处理，同时考虑到成员国法律可制定关于数据保护的特定规定，以使本条例规则的适用符合法律义务，或为履行公共利益任务或行使赋予控制者的官方职权。除对此类处理的特定要求外，本条例的一般原则和其他规则应适用，特别是关于合法处理条件的规定。对此类特殊类别个人数据处理的一般禁止的例外应明确规定，除其他外，在数据主体给予其明确同意的情况下，或针对特定需要，特别是在某些协会或基金会为允许行使基本自由而开展的正当活动过程中进行处理的情况下。

(52) Derogating from the prohibition on processing special categories of personal data should also be allowed when provided for in Union or Member State law and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where it is in the public interest to do so, in particular processing personal data in the field of employment law, social protection law including pensions and for health security, monitoring and alert purposes, the prevention or control of communicable diseases and other serious threats to health. Such a derogation may be made for health purposes, including public health and the management of health-care services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. A derogation should also allow the processing of such personal data where necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure.

(52) 当联盟或成员国法律有规定并受适当保障措施约束时，也应当允许对处理特殊类别的个人数据的禁令作出例外，以便在符合公共利益的情况下保护个人数据和其他基本权利，特别是在劳动法、社会保障法(包括养老金)以及健康安全、监测和预警目的、预防或控制传染病和其他严重健康威胁领域处理个人数据。此种例外可为健康目的而作出，包括公共卫生和医疗保健服务的管理，特别是为了确保在健康保险制度中处理福利和服务索赔所用程序的质量和成本效益，或为公共利益存档目的、科学或历史研究目的或统计目的而作出。例外还应当允许在为确立、行使或抗辩法律主张所必需时处理此类个人数据，无论是在法院诉讼中还是在行政或庭外程序中。

(53) Special categories of personal data which merit higher protection should be processed for health-related purposes only where necessary to achieve those purposes for the benefit of natural persons and society as a whole, in particular in the context of the management of health or social care services and systems, including processing by the management and central national health authorities of such data for the purpose of quality control, management information and the general national and local supervision of the health or social care system, and ensuring continuity of health or social care and cross-border healthcare or health security, monitoring and alert purposes, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, based on Union or Member State law which has to meet an objective of public interest, as well as for studies conducted in the public interest in the area of public health. Therefore, this Regulation should provide for harmonised conditions for the processing of special categories of personal data concerning health, in respect of specific needs, in particular where the processing of such data is carried out for certain health-related purposes

(53) 值得更高保护的特殊类别的个人数据，应当仅为实现有利于自然人和整个社会的健康相关目的所必需时予以处理，特别是在健康或社会照护服务及系统的管理背景下，包括由管理层和国家中央卫生主管部门为此类数据的质量控制、管理信息以及对健康或社会照护系统的一般国家和地方监督之目的进行处理，以及确保健康或社会照护的连续性以及跨境医疗保健或健康安全、监测和预警目的，或为公共利益存档目的、科学或历史研究目的或统计目的，依据必须符合公共利益目标的联盟或成员国法律进行处理，以及为公共卫生领域符合公共利益的研究而进行处理。因此，本条例应当针对特定需求，为处理与健康有关的特殊类别的个人数据规定统一的条件，特别是在此类数据的处理系由承担职业保密法律义务的人员为某些健康相关目的而进行的情况下。

by persons subject to a legal obligation of professional secrecy. Union or Member State law should provide for specific and suitable measures so as to protect the fundamental rights and the personal data of natural persons. Member States should be allowed to maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health. However, this should not hamper the free flow of personal data within the Union when those conditions apply to cross-border processing of such data.

(54) The processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject. Such processing should be subject to suitable and specific measures so as to protect the rights and freedoms of natural persons. In that context, 'public health' should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council ([1]), namely all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. Such processing of data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers or insurance and banking companies.

(55) Moreover, the processing of personal data by official authorities for the purpose of achieving the aims, laid down by constitutional law or by international public law, of officially recognised religious associations, is carried out on grounds of public interest.

(56) Where in the course of electoral activities, the operation of the democratic system in a Member State requires that political parties compile personal data on people's political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established.

(57) If the personal data processed by a controller do not permit the controller to identify a natural person, the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation. However, the controller should not refuse to take additional information provided by the data subject in order to support the exercise of his or her rights. Identification should include the digital identification of a data subject, for example through authentication mechanism such as the same credentials, used by the data subject to log-in to the on-line service offered by the data controller.

(58) The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used. Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising. Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.

(59) Modalities should be provided for facilitating the exercise of the data subject's rights under this Regulation, including mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and the exercise of the right to object. The controller should also provide means for requests to be made electronically, especially where personal data are processed by electronic means. The controller should be obliged to respond to requests from the data subject without undue delay and at the latest within one month and to give reasons where the controller does not intend to comply with any such requests.

([1]) Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work (OJ L 354, 31.12.2008, p. 70).

联盟或成员国法律应当规定具体和适当的措施，以保护自然人的基本权利和个人数据。应当允许成员国就基因数据、生物识别数据或与健康有关的数据的处理维持或引入进一步的条件，包括限制。但是，当这些条件适用于此类数据的跨境处理时，不应妨碍个人数据在联盟内的自由流动。

(54) 在公共卫生领域，为公共利益的原因，可能需要在未经数据主体同意的情况下处理特殊类别的个人数据。此种处理应当受到适当和具体措施的约束，以保护自然人的权利和自由。在此背景下，“公共卫生”应当按照欧洲议会和理事会第(EC) No 1338/2008号条例(1)中的定义加以解释，即与健康有关的所有要素，即健康状况，包括发病率和残疾情况、影响该健康状况的决定因素、医疗保健需求、分配给医疗保健的资源、医疗保健的提供和普遍可及性以及医疗保健支出和筹资，以及死亡原因。此种为公共利益原因处理与健康有关的数据，不应导致第三方(如雇主或保险和银行公司)为其他目的处理个人数据。

(55) 此外，官方当局为实现官方认可的宗教协会依宪法或国际公法所规定的宗旨而进行的个人数据处理，是基于公共利益进行的。

(56) 在选举活动过程中，若成员国的民主制度运行要求政党汇编关于人们政治观点的个人数据，则可基于公共利益理由允许处理此类数据，前提是建立了适当保障措施。

(57) 如果控制者处理的个人数据不允许控制者识别自然人，则不应仅为遵守本条例任何规定之目的而要求数据控制者获取额外信息以识别数据主体。但是，控制者不应拒绝接收数据主体为支持行使其权利而提供的额外信息。识别应当包括对数据主体的数字识别，例如通过认证机制，如数据主体用于登录数据控制者所提供的在线服务的相同凭据。

(58) 透明原则要求，任何面向公众或数据主体的信息应当简明、易于获取且易于理解，并应使用清晰平实的语言，此外在适当情况下还应使用可视化方式。此类信息可以电子形式提供，例如在面向公众时通过网站提供。在行为主体众多且实践的技术复杂性使数据主体难以知晓和理解与其相关的个人数据是否正在被收集、由谁收集以及出于何种目的收集的情况下，例如在线广告的情形，这一点尤为重要。鉴于儿童值得特殊保护，当处理涉及儿童时，任何信息和通信应当使用儿童能够轻易理解的清晰平实语言。

(59) 应当规定便利数据主体行使本条例下权利的方式，包括请求并在适用情况下免费获得特别是个人数据的访问、更正或删除以及行使反对权的机制。控制者还应当提供以电子方式提出请求的手段，特别是在个人数据通过电子方式处理的情况下。控制者有义务无不当延迟地回应数据主体的请求，最迟在一个月内作出回应，并在控制者不打算遵从任何此类请求时说明理由。

(1) 2008年12月16日欧洲议会和理事会关于公共卫生及工作场所健康与安全共同体统计的第1338/2008号条例(EC)(OJ L 354, 31.12.2008, p.70)。

(60) The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed. Furthermore, the data subject should be informed of the existence of profiling and the consequences of such profiling. Where the personal data are collected from the data subject, the data subject should also be informed whether he or she is obliged to provide the personal data and of the consequences, where he or she does not provide such data. That information may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing. Where the icons are presented electronically, they should be machine-readable.

(61) The information in relation to the processing of personal data relating to the data subject should be given to him or her at the time of collection from the data subject, or, where the personal data are obtained from another source, within a reasonable period, depending on the circumstances of the case. Where personal data can be legitimately disclosed to another recipient, the data subject should be informed when the personal data are first disclosed to the recipient. Where the controller intends to process the personal data for a purpose other than that for which they were collected, the controller should provide the data subject prior to that further processing with information on that other purpose and other necessary information. Where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided.

(62) However, it is not necessary to impose the obligation to provide information where the data subject already possesses the information, where the recording or disclosure of the personal data is expressly laid down by law or where the provision of information to the data subject proves to be impossible or would involve a disproportionate effort. The latter could in particular be the case where processing is carried out for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. In that regard, the number of data subjects, the age of the data and any appropriate safeguards adopted should be taken into consideration.

(63) A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing. This includes the right for data subjects to have access to data concerning their health, for example the data in their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided. Every data subject should therefore have the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing. Where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data. That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject. Where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates.

(64) The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests.

(65) A data subject should have the right to have personal data concerning him or her rectified and a 'right to be forgotten' where the retention of such data infringes this Regulation or Union or Member State law to which the controller is subject. In particular, a data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation. That right is relevant in particular where the data subject has given

(60) 公平和透明处理原则要求数据主体被告知处理操作的存在及其目的。控制者应当向数据主体提供为确保公平和透明处理所必需的任何进一步信息，同时考虑个人数据处理的具体情形和背景。此外，数据主体应当被告知画像的存在及其后果。在个人数据从数据主体处收集的情况下，数据主体还应当被告知是否有义务提供个人数据以及不提供此类数据的后果。该信息可以结合标准化图标提供，以便以易于看见、可理解和清晰可读的方式对所预期的处理提供有意义的概览。在图标以电子方式呈现的情况下，图标应当机器可读。

(61) 与处理数据主体相关个人数据有关的信息应当在从数据主体处收集时向其提供，或者在个人数据从另一来源获得的情况下，在合理期限内提供，具体取决于案件情形。在个人数据可以合法披露给另一接收方的情况下，数据主体应当在个人数据首次披露给该接收方时被告知。在控制者意图将个人数据用于收集目的之外的其他目的进行处理的情况下，控制者应当在该进一步处理之前向数据主体提供关于该其他目的的信息及其他必要信息。在因使用了多种来源而无法向数据主体提供个人数据来源的情况下，应当提供一般性信息。

(62) 然而，在数据主体已经拥有该信息、个人数据的记录或披露由法律明确规定、或者向数据主体提供信息被证明不可能或会涉及不成比例的努力的情况下，无需施加提供信息的义务。后一种情况尤其可能出现在为公共利益存档目的、科学或历史研究目的或统计目的进行处理的情形。在这方面，应当考虑数据主体的数量、数据的年代以及所采取的任何适当保障措施。

(63) 数据主体应当有权访问已收集的与其有关的个人数据，并有权以合理的间隔便捷地行使该权利，以便知悉并核实处理的合法性。这包括数据主体有权访问与其健康有关的数据，例如其医疗记录中包含诊断、检查结果、主治医师的评估以及所提供的任何治疗或干预等信息的数据。因此，每个数据主体都应有权知悉并获取通知，特别是关于处理个人数据的目的、在可能的情况下处理个人数据的期限、个人数据的接收方、任何自动化个人数据处理所涉及的逻辑，以及至少在以画像为基础时此类处理所产生的后果。在可能的情况下，控制者应当能够提供对安全系统的远程访问，使数据主体能够直接访问其个人数据。该权利不应对他人的权利或自由产生不利影响，包括商业秘密或知识产权，特别是保护软件的版权。然而，这些考量不应导致拒绝向数据主体提供全部信息。当控制者处理大量与数据主体有关的信息时，控制者应当能够要求在信息交付之前，由数据主体指明该请求所涉及的信息或处理活动。

(64) 控制者应采取一切合理措施核实请求访问的数据主体的身份，特别是在在线服务和在线标识符的背景下。控制者不应仅为能够回应潜在请求而保留个人数据。

(65) 数据主体应当有权更正与其有关的个人数据，并在保留此类数据违反本条例或控制者所受约束的联盟或成员国法律的情况下，享有"被遗忘权"。特别是，在个人数据对于其被收集或以其他方式处理的目的而言已不再必要、数据主体已撤回其同意或反对处理与其有关的个人数据、或者处理其个人数据在其他方面不符合本条例的情况下，数据主体应当有权要求删除其个人数据并且不再被处理。该权利在以下情形尤其相关：数据主体在儿童时期已给出

his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child. However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims.

(66) To strengthen the right to be forgotten in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform the controllers which are processing such personal data to erase any links to, or copies or replications of those personal data. In doing so, that controller should take reasonable steps, taking into account available technology and the means available to the controller, including technical measures, to inform the controllers which are processing the personal data of the data subject's request.

(67) Methods by which to restrict the processing of personal data could include, inter alia, temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website. In automated filing systems, the restriction of processing should in principle be ensured by technical means in such a manner that the personal data are not subject to further processing operations and cannot be changed. The fact that the processing of personal data is restricted should be clearly indicated in the system.

(68) To further strengthen the control over his or her own data, where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller. Data controllers should be encouraged to develop interoperable formats that enable data portability. That right should apply where the data subject provided the personal data on the basis of his or her consent or the processing is necessary for the performance of a contract. It should not apply where processing is based on a legal ground other than consent or contract. By its very nature, that right should not be exercised against controllers processing personal data in the exercise of their public duties. It should therefore not apply where the processing of the personal data is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller. The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible. Where, in a certain set of personal data, more than one data subject is concerned, the right to receive the personal data should be without prejudice to the rights and freedoms of other data subjects in accordance with this Regulation. Furthermore, that right should not prejudice the right of the data subject to obtain the erasure of personal data and the limitations of that right as set out in this Regulation and should, in particular, not imply the erasure of personal data concerning the data subject which have been provided by him or her for the performance of a contract to the extent that and for as long as the personal data are necessary for the performance of that contract. Where technically feasible, the data subject should have the right to have the personal data transmitted directly from one controller to another.

(69) Where personal data might lawfully be processed because processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, or on grounds of the legitimate interests of a controller or a third party, a data subject should, nevertheless, be entitled to object to the processing of any personal data relating to his or her particular situation. It should be for the controller to demonstrate that its compelling legitimate interest overrides the interests or the fundamental rights and freedoms of the data subject.

(70) Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing, including profiling to the extent that it is related to such direct marketing, whether with regard to initial or further processing, at any time and free of charge. That right should be explicitly brought to the attention of the data subject and presented clearly and separately from any other information.

其同意，且并未充分意识到处理所涉及的风险，而后希望删除此类个人数据，尤其是在互联网上。数据主体应当能够行使该权利，即使其已不再是儿童。然而，在为行使表达和信息自由权、为遵守法律义务、为执行为公共利益而执行的任务或为行使赋予控制者的官方职权所必需、基于公共卫生领域的公共利益、为公共利益存档目的、科学或历史研究目的或统计目的、或者为确立、行使或抗辩法律主张所必需的情况下，进一步保留个人数据应当是合法的。

(66) 为加强在线环境中的被遗忘权，删除权还应扩展至：已公开个人数据的控制者应当有义务通知正在处理此类个人数据的控制者删除指向这些个人数据的任何链接，或删除这些个人数据的副本或复制件。在这样做时，该控制者应当采取合理步骤，考虑现有技术和控制者可用的手段，包括技术措施，将数据主体的请求告知正在处理个人数据的控制者。

(67) 限制处理个人数据的方法可以包括：将所选数据临时移至另一处理系统、使所选个人数据对用户不可用、或临时从网站移除已发布的数据等。在自动化档案系统中，限制处理原则上应当通过技术手段予以确保，使得个人数据不受进一步处理操作的影响且不能被更改。个人数据处理受到限制这一事实应当在系统中明确标示。

(68) 为进一步加强对自身数据的控制，在个人数据通过自动化方式处理的情况下，还应允许数据主体以结构化、常用、机器可读和可互操作的格式接收其已提供给控制者的与其有关的个人数据，并将其传输给另一控制者。应鼓励数据控制者开发可实现数据可携带权的可互操作格式。该权利应适用于数据主体基于其同意提供个人数据或处理对于履行合同所必需的情形。它不应适用于处理基于同意或合同以外的法律依据的情形。就其本质而言，该权利不应针对在履行公共职责时处理个人数据的控制者行使。因此，它不应适用于为遵守控制者所承担的法律义务或为执行以公共利益为目的的任务或行使赋予控制者的官方职权而处理个人数据所必需的情形。数据主体传输或接收与其有关的个人数据的权利不应为控制者创设采用或维护技术上兼容的处理系统的义务。在某一组个人数据涉及不止一个数据主体的情况下，接收个人数据的权利不应损害其他数据主体依照本条例享有的权利和自由。此外，该权利不应损害数据主体获得个人数据擦除的权利以及本条例所规定的对该权利的限制，尤其不应意味着擦除数据主体为履行合同而提供的与其有关的个人数据，只要且仅在该个人数据对于履行该合同所必需的范围内。在技术可行的情况下，数据主体应有权将个人数据从一个控制者直接传输至另一控制者。

(69) 在因处理对于执行以公共利益为目的的任务或行使赋予控制者的官方职权所必需，或基于控制者或第三方的正当利益而可以合法处理个人数据的情况下，数据主体仍应有权反对处理与其特定情形有关的任何个人数据。控制者应证明其令人信服的正当利益优先于数据主体的利益或基本权利和自由。

(70) 为直接营销目的处理个人数据时，数据主体应有权随时免费反对此类处理，包括与此类直接营销相关的画像，无论是初始处理还是进一步处理。该权利应明确提请数据主体注意，并清晰呈现，与任何其他信息分开。

(71) The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention. Such processing includes 'profiling' that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her. However, decision-making based on such processing, including profiling, should be allowed where expressly authorised by Union or Member State law to which the controller is subject, including for fraud and tax-evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller, or necessary for the entering or performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit consent. In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. Such measure should not concern a child.

In order to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal data are processed, the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect. Automated decision-making and profiling based on special categories of personal data should be allowed only under specific conditions.

(72) Profiling is subject to the rules of this Regulation governing the processing of personal data, such as the legal grounds for processing or data protection principles. The European Data Protection Board established by this Regulation (the 'Board') should be able to issue guidance in that context.

(73) Restrictions concerning specific principles and the rights of information, access to and rectification or erasure of personal data, the right to data portability, the right to object, decisions based on profiling, as well as the communication of a personal data breach to a data subject and certain related obligations of the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of human life especially in response to natural or manmade disasters, the prevention, investigation and prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, or of breaches of ethics for regulated professions, other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, the keeping of public registers kept for reasons of general public interest, further processing of archived personal data to provide specific information related to the political behaviour under former totalitarian state regimes or the protection of the data subject or the rights and freedoms of others, including social protection, public health and humanitarian purposes. Those restrictions should be in accordance with the requirements set out in the Charter and in the European Convention for the Protection of Human Rights and Fundamental Freedoms.

(74) The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.

(71) 数据主体应有权不受仅基于自动化处理(包括评估与其有关的个人方面)且对其产生法律效力或类似重大影响的决定(可包括措施)的约束，例如在无任何人工干预的情况下自动拒绝在线信贷申请或电子招聘做法。此类处理包括"画像"，即任何形式的个人数据自动化处理，用以评估与自然人有关的个人方面，特别是分析和预测与数据主体的工作表现、经济状况、健康、个人偏好或利益、可靠性或行为、位置或移动有关的方面，且该处理对其产生法律效力或类似重大影响。然而，在控制者所适用的Union或成员国法律明确授权的情况下，包括为依照Union机构或国家监督机构的法规、标准和建议进行欺诈和逃税监测和预防之目的，以及为确保控制者所提供服务的安全性和可靠性，或为数据主体与控制者之间订立或履行合同所必需，或数据主体已给予其明确同意的情况下，应允许基于此类处理(包括画像)作出决策。在任何情况下，此类处理均应受到适当保障措施的约束，其中应包括向数据主体提供具体信息以及获得人工干预、表达其观点、获得对此类评估后所作决定的解释并对该决定提出质疑的权利。此类措施不应涉及儿童。

为确保对数据主体的公平和透明处理，考虑到处理个人数据的具体情形和背景，控制者应使用适当的数学或统计程序进行画像，实施适当的技术和组织措施，以确保特别是纠正导致个人数据不准确的因素并将错误风险降至最低，以考虑到对数据主体的利益和权利所涉潜在风险的方式保护个人数据，并尤其防止基于种族或民族出身、政治观点、宗教或信仰、工会成员身份、遗传或健康状况或性取向对自然人产生歧视性影响，或防止导致具有此类影响的措施。仅应在特定条件下才允许基于特殊类别的个人数据进行自动化决策和画像。

(72) 画像受本条例关于个人数据处理规则的约束，例如处理的法律依据或数据保护原则。依本条例设立的欧洲数据保护委员会("委员会")应能够就此发布指导意见。

(73) 有关特定原则以及信息权、个人数据访问权和更正或擦除权、数据可携带权、反对权、基于画像的决定，以及向数据主体告知个人数据泄露和控制者某些相关义务的限制，可由Union或成员国法律施加，只要在民主社会中为保障公共安全所必需且相称，包括保护人的生命，特别是应对自然或人为灾害，预防、调查和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，或违反受监管职业的道德规范，Union或成员国的其他一般公共利益的重要目标，特别是Union或成员国的重要经济或金融利益，为一般公共利益原因而保存的公共登记册的保存，为提供与前极权国家制度下政治行为有关的特定信息而对存档个人数据进行的进一步处理，或对数据主体或他人权利和自由的保护，包括社会保护、公共卫生和人道主义目的。这些限制应符合《宪章》和《欧洲人权与基本自由公约》所规定的要求。

(74) 应确立控制者对由控制者或代表控制者进行的任何个人数据处理的责任和义务。特别是，控制者应有义务实施适当和有效的措施，并能够证明处理活动符合本条例，包括措施的有效性。这些措施应考虑处理的性质、范围、背景和目的以及对自然人权利和自由的风险。

(75) The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.

(76) The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk.

(77) Guidance on the implementation of appropriate measures and on the demonstration of compliance by the controller or the processor, especially as regards the identification of the risk related to the processing, their assessment in terms of origin, nature, likelihood and severity, and the identification of best practices to mitigate the risk, could be provided in particular by means of approved codes of conduct, approved certifications, guidelines provided by the Board or indications provided by a data protection officer. The Board may also issue guidelines on processing operations that are considered to be unlikely to result in a high risk to the rights and freedoms of natural persons and indicate what measures may be sufficient in such cases to address such risk.

(78) The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders.

(79) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors, also in relation to the monitoring by and measures of supervisory authorities, requires a clear allocation of the responsibilities under this Regulation, including where a controller determines the purposes and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.

(80) Where a controller or a processor not established in the Union is processing personal data of data subjects who are in the Union whose processing activities are related to the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union, or to the monitoring of their behaviour as far as their behaviour takes place within the Union, the controller or the processor should designate a representative, unless the processing is occasional, does not include processing, on a large scale, of special categories of personal data or the processing of personal data relating to criminal convictions and offences, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the

(75) 对自然人权利和自由的风险，其可能性和严重程度各不相同，可能源于个人数据处理，这些处理可能导致身体、物质或非物质损害，特别是：处理可能引发歧视、身份盗窃或欺诈、经济损失、名誉损害、受职业保密保护的个人数据机密性丧失、假名化的未经授权逆转或任何其他重大经济或社会不利影响；数据主体可能被剥夺其权利和自由或被阻止对其个人数据行使控制；处理揭示种族或民族出身、政治观点、宗教或哲学信仰、工会成员身份的个人数据，以及处理遗传数据、健康数据或有关性生活或刑事定罪和犯罪或相关安全措施的数据；对个人方面进行评估，特别是分析和预测有关工作表现、经济状况、健康、个人偏好或兴趣、可靠性或行为、位置或移动方面，以创建或使用个人画像；处理弱势自然人特别是儿童的个人数据；或处理涉及大量个人数据并影响大量数据主体。

(76) 数据主体权利和自由所面临风险的可能性和严重性应参照处理的性质、范围、背景和目的来确定。风险应基于客观评估进行评价，据此确定数据处理操作是否涉及风险或高风险。

(77) 关于实施适当措施和证明控制者或处理者合规的指导，特别是关于识别与处理相关的风险、按其来源、性质、可能性和严重程度进行评估，以及识别缓解风险的最佳实践，可特别通过经批准的行为准则、经批准的认证、委员会提供的指南或数据保护官提供的指示来提供。委员会还可就认为不太可能导致对自然人权利和自由的高风险的处理操作发布指南，并指明在此类情况下哪些措施可能足以应对此类风险。

(78) 在个人数据处理方面保护自然人的权利和自由要求采取适当的技术和组织措施，以确保满足本条例的要求。为了能够证明符合本条例，控制者应采纳内部政策并实施特别符合数据保护设计和默认数据保护原则的措施。此类措施可包括：最小化个人数据处理、尽快假名化个人数据、在个人数据的功能和处理方面保持透明、使数据主体能够监控数据处理、使控制者能够创建和改进安全功能。在开发、设计、选择和使用基于个人数据处理或处理个人数据以完成其任务的应用程序、服务和产品时，应鼓励产品、服务和应用程序的生产者在开发和设计此类产品、服务和应用程序时考虑数据保护权，并在适当考虑最新技术水平的情况下，确保控制者和处理者能够履行其数据保护义务。在公共招标的背景下，也应考虑数据保护设计和默认数据保护原则。

(79) 保护数据主体的权利和自由以及控制者和处理者的责任和法律责任(包括在监管机构的监督和措施方面)，要求根据本条例明确分配责任，包括控制者与其他控制者共同确定处理的目的和方式，或处理操作代表控制者进行的情形。

(80) 未在欧盟设立的控制者或处理者处理在欧盟内的数据主体的个人数据，其处理活动涉及向欧盟内的此类数据主体提供商品或服务(无论是否要求数据主体付款)，或监控其行为(只要其行为发生在欧盟内)，控制者或处理者应指定一名代表，除非处理是偶尔的、不涉及大规模处理特殊类别的个人数据或处理与刑事定罪和犯罪有关的个人数据，并且不太可能导致对自然人权利和自由的风险，同时考虑到

nature, context, scope and purposes of the processing or if the controller is a public authority or body. The representative should act on behalf of the controller or the processor and may be addressed by any supervisory authority. The representative should be explicitly designated by a written mandate of the controller or of the processor to act on its behalf with regard to its obligations under this Regulation. The designation of such a representative does not affect the responsibility or liability of the controller or of the processor under this Regulation. Such a representative should perform its tasks according to the mandate received from the controller or processor, including cooperating with the competent supervisory authorities with regard to any action taken to ensure compliance with this Regulation. The designated representative should be subject to enforcement proceedings in the event of non-compliance by the controller or processor.

处理的性质、背景、范围和目的，或者控制者是否为公共机关或机构。代表应代表控制者或处理者行事，任何监管机构均可向其提出事项。代表应由控制者或处理者通过书面授权明确指定，代表其履行本条例规定的义务。指定此类代表不影响控制者或处理者在本条例下的责任或义务。此类代表应根据控制者或处理者授予的授权执行任务，包括与主管监管机构合作，就为确保遵守本条例而采取的任何行动进行配合。如果控制者或处理者不遵守规定，被指定的代表应受到执法程序的约束。

(81) To ensure compliance with the requirements of this Regulation in respect of the processing to be carried out by the processor on behalf of the controller, when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of this Regulation, including for the security of processing. The adherence of the processor to an approved code of conduct or an approved certification mechanism may be used as an element to demonstrate compliance with the obligations of the controller. The carrying-out of processing by a processor should be governed by a contract or other legal act under Union or Member State law, binding the processor to the controller, setting out the subject-matter and duration of the processing, the nature and purposes of the processing, the type of personal data and categories of data subjects, taking into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk to the rights and freedoms of the data subject. The controller and processor may choose to use an individual contract or standard contractual clauses which are adopted either directly by the Commission or by a supervisory authority in accordance with the consistency mechanism and then adopted by the Commission. After the completion of the processing on behalf of the controller, the processor should, at the choice of the controller, return or delete the personal data, unless there is a requirement to store the personal data under Union or Member State law to which the processor is subject.

(81) 为确保在处理者代表控制者开展处理活动时遵守本条例的要求，控制者在委托处理者开展处理活动时，应仅使用能够提供充分保证的处理者，特别是在专业知识、可靠性和资源方面，以实施符合本条例要求的技术和组织措施，包括处理安全方面的措施。处理者遵守经批准的行为准则或经批准的认证机制，可作为证明控制者履行义务的一个要素。处理者开展处理活动应由根据联盟法或成员国法律签订的合同或其他法律行为管辖，该合同或法律行为对处理者具有约束力并约束控制者，规定处理的主题事项和持续时间、处理的性质和目的、个人数据的类型和数据主体的类别，同时考虑处理者在拟开展处理活动背景下的具体任务和责任，以及对数据主体权利和自由的风险。控制者和处理者可以选择使用单独合同或标准合同条款，这些标准合同条款由委员会直接通过，或由监管机构根据一致性机制通过后由委员会通过。在代表控制者完成处理后，处理者应根据控制者的选择，返还或删除个人数据，除非处理者所受管辖的联盟法或成员国法律要求存储该个人数据。

(82) In order to demonstrate compliance with this Regulation, the controller or processor should maintain records of processing activities under its responsibility. Each controller and processor should be obliged to cooperate with the supervisory authority and make those records, on request, available to it, so that it might serve for monitoring those processing operations.

(82) 为证明遵守本条例，控制者或处理者应保存其负责下的处理活动记录。每个控制者和处理者都有义务与监管机构合作，并应要求向其提供这些记录，以便其可用于监督这些处理操作。

(83) In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.

(83) 为了维护安全并防止违反本条例的处理活动，控制者或处理者应评估处理中固有的风险，并实施减轻这些风险的措施，例如加密。这些措施应确保适当的安全水平，包括保密性，同时考虑现有技术水平、实施成本与风险以及受保护个人数据的性质之间的关系。在评估数据安全风险时，应考虑个人数据处理所带来的风险，例如意外或非法的破坏、丢失、更改、未经授权的披露或访问传输、存储或以其他方式处理的个人数据，这些风险尤其可能导致物理、物质或非物质损害。

(84) In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk. The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation. Where a data-protection impact assessment indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing.

(84) 为了在处理操作可能对自然人的权利和自由造成高风险的情况下加强对本条例的遵守，控制者应负责开展数据保护影响评估，以特别评估该风险的来源、性质、特殊性和严重性。在确定应采取适当措施以证明个人数据处理符合本条例时，应考虑评估结果。如果数据保护影响评估表明处理操作涉及控制者无法通过现有技术和实施成本方面的适当措施减轻的高风险，则应在处理前咨询监管机构。

(85) A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned. Therefore, as soon as the controller becomes

(85) 个人数据泄露如果未得到适当和及时的处理，可能对自然人造成物理、物质或非物质损害，例如失去对其个人数据的控制或权利受限、歧视、身份盗窃或欺诈、经济损失、假名化的未经授权逆转、名誉损害、受职业保密保护的个人数据失去保密性，或对相关自然人造成任何其他重大经济或社会不利影响。因此，一旦控制者得知

aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay.

(86) The controller should communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person in order to allow him or her to take the necessary precautions. The communication should describe the nature of the personal data breach as well as recommendations for the natural person concerned to mitigate potential adverse effects. Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities. For example, the need to mitigate an immediate risk of damage would call for prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication.

(87) It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject. The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation.

(88) In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of that breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse. Moreover, such rules and procedures should take into account the legitimate interests of law-enforcement authorities where early disclosure could unnecessarily hamper the investigation of the circumstances of a personal data breach.

(89) Directive 95/46/EC provided for a general obligation to notify the processing of personal data to the supervisory authorities. While that obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Such indiscriminate general notification obligations should therefore be abolished, and replaced by effective procedures and mechanisms which focus instead on those types of processing operations which are likely to result in a high risk to the rights and freedoms of natural persons by virtue of their nature, scope, context and purposes. Such types of processing operations may be those which in, particular, involve using new technologies, or are of a new kind and where no data protection impact assessment has been carried out before by the controller, or where they become necessary in the light of the time that has elapsed since the initial processing.

(90) In such cases, a data protection impact assessment should be carried out by the controller prior to the processing in order to assess the particular likelihood and severity of the high risk, taking into account the nature, scope, context and purposes of the processing and the sources of the risk. That impact assessment should include, in particular, the measures, safeguards and mechanisms envisaged for mitigating that risk, ensuring the protection of personal data and demonstrating compliance with this Regulation.

(91) This should in particular apply to large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk, for example, on account of their sensitivity, where in accordance with the achieved state of technological knowledge a new technology is used on a large scale as well as to other processing operations which result in a high risk to the rights and freedoms of data subjects, in particular where those operations render it more difficult for data subjects to exercise their rights. A data

控制者一旦知晓个人数据泄露，应当毫不迟延地通知监管机构，并在可行的情况下，最迟在知晓后 72 小时内通知，除非控制者能够依据问责原则证明该个人数据泄露不太可能导致自然人的权利和自由面临风险。如果无法在 72 小时内完成此类通知，应当随通知说明延迟的理由，并可以在不造成进一步不当延迟的情况下分阶段提供信息。

(86) 如果个人数据泄露很可能对自然人的权利和自由造成高风险，控制者应当毫不迟延地将该个人数据泄露告知数据主体，以便其采取必要预防措施。该告知应当描述个人数据泄露的性质，并向相关自然人提出减轻潜在不利影响的建议。此类向数据主体的告知应当在合理可行的情况下尽快进行，并与监管机构密切合作，遵守监管机构或其他相关机构(如执法机构)提供的指导。例如，减轻即时损害风险的需要要求迅速与数据主体沟通，而针对持续或类似个人数据泄露实施适当措施的需要则可能为沟通留出更多时间。

(87) 应当查明是否已实施所有适当的技术保护和组织措施，以便立即确定是否发生了个人数据泄露，并及时通知监管机构和数据主体。确定通知是否毫不迟延，应当特别考虑个人数据泄露的性质和严重程度及其对数据主体的后果和不利影响。此类通知可能导致监管机构依据本条例规定的任务和权力进行干预。

(88) 在制定关于个人数据泄露通知的格式和程序的详细规则时，应当适当考虑该泄露的具体情况，包括个人数据是否受到适当技术保护措施的保护，从而有效降低身份欺诈或其他形式滥用的可能性。此外，此类规则和程序应当考虑执法机构的正当利益，因为过早披露可能不必要地妨碍对个人数据泄露情况的调查。

(89) Directive 95/46/EC 规定了向监管机构通知个人数据处理的一般义务。该义务虽然带来行政和财务负担，但并非在所有情况下都有助于改善个人数据保护。因此，应当废除此类不加区分的一般通知义务，并以有效的程序和机制取而代之，转而重点关注那些因其性质、范围、背景和目的而很可能对自然人的权利和自由造成高风险的处理操作类型。此类处理操作类型尤其可能包括使用新技术的操作，或属于新类型且控制者此前未进行数据保护影响评估的操作，或鉴于自初始处理以来经过的时间而变得必要的操作。

(90) 在此类情况下，控制者应当在处理之前进行数据保护影响评估，以便在考虑处理的性质、范围、背景和目的以及风险来源的基础上，评估高风险的具体可能性和严重程度。该影响评估尤其应当包括为减轻该风险、确保个人数据的保护以及证明符合本条例而设想采取的措施、保障和机制。

(91) 这尤其应当适用于大规模处理操作，其目的在于在区域、国家或超国家层面处理大量个人数据，可能影响大量数据主体，并且很可能导致高风险，例如由于其敏感性，根据已达到的技术知识水平大规模使用新技术，以及适用于其他导致数据主体的权利和自由面临高风险的处理操作，特别是当这些操作使数据主体更难行使其权利时。数据

protection impact assessment should also be made where personal data are processed for taking decisions regarding specific natural persons following any systematic and extensive evaluation of personal aspects relating to natural persons based on profiling those data or following the processing of special categories of personal data, biometric data, or data on criminal convictions and offences or related security measures. A data protection impact assessment is equally required for monitoring publicly accessible areas on a large scale, especially when using optic-electronic devices or for any other operations where the competent supervisory authority considers that the processing is likely to result in a high risk to the rights and freedoms of data subjects, in particular because they prevent data subjects from exercising a right or using a service or a contract, or because they are carried out systematically on a large scale. The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer. In such cases, a data protection impact assessment should not be mandatory.

(92) There are circumstances under which it may be reasonable and economical for the subject of a data protection impact assessment to be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity.

(93) In the context of the adoption of the Member State law on which the performance of the tasks of the public authority or public body is based and which regulates the specific processing operation or set of operations in question, Member States may deem it necessary to carry out such assessment prior to the processing activities.

(94) Where a data protection impact assessment indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation, the supervisory authority should be consulted prior to the start of processing activities. Such high risk is likely to result from certain types of processing and the extent and frequency of processing, which may result also in a realisation of damage or interference with the rights and freedoms of the natural person. The supervisory authority should respond to the request for consultation within a specified period. However, the absence of a reaction of the supervisory authority within that period should be without prejudice to any intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation, including the power to prohibit processing operations. As part of that consultation process, the outcome of a data protection impact assessment carried out with regard to the processing at issue may be submitted to the supervisory authority, in particular the measures envisaged to mitigate the risk to the rights and freedoms of natural persons.

(95) The processor should assist the controller, where necessary and upon request, in ensuring compliance with the obligations deriving from the carrying out of data protection impact assessments and from prior consultation of the supervisory authority.

(96) A consultation of the supervisory authority should also take place in the course of the preparation of a legislative or regulatory measure which provides for the processing of personal data, in order to ensure compliance of the intended processing with this Regulation and in particular to mitigate the risk involved for the data subject.

(97) Where the processing is carried out by a public authority, except for courts or independent judicial authorities when acting in their judicial capacity, where, in the private sector, processing is carried out by a controller whose core activities consist of processing operations that require regular and systematic monitoring of the data subjects on a large scale, or where the core activities of the controller or the processor consist of processing on a large scale of special categories of personal data and data relating to criminal convictions and offences, a person with expert knowledge of data protection law and practices should assist the controller or processor to monitor internal compliance with this Regulation. In the private sector, the core activities of a controller relate to its primary activities and do not relate to the processing of personal data as ancillary activities. The necessary level of expert knowledge should be determined in particular according to the data processing operations carried out

保护影响评估也应当在进行以下处理时进行：基于对这些数据的画像或在对特殊类别的个人数据、生物识别数据或关于刑事定罪和犯罪或相关安全措施的数据进行处理之后，对与自然人有关的个人方面进行任何系统性和广泛性评估后，为作出关于特定自然人的决定而处理个人数据。对于大规模监控可公开访问区域，特别是使用光电设备时，或对于主管监管机构认为处理很可能对数据主体的权利和自由造成高风险的任何其他操作，特别是因为这些操作阻止数据主体行使权利或使用服务或合同，或因为这些操作是系统性地大规模进行的，同样需要进行数据保护影响评估。如果处理涉及个别医生、其他医疗保健专业人员或律师对患者或客户的个人数据的处理，则不应当视为大规模处理。在此类情况下，数据保护影响评估不应当是强制性的。

(92) 在某些情况下，数据保护影响评估的主题比单个项目更广泛可能是合理且经济的，例如公共当局或机构打算建立共同的应用或处理平台，或者若干控制者计划在整个行业部门或细分领域或针对广泛使用的横向活动引入共同的应用或处理环境。

(93) 在通过成员国法律(公共当局或公共机构履行任务所依据并规范特定处理操作或相关操作集合的法律)的背景下，成员国可认为有必要在处理活动之前进行此类评估。

(94) 如果数据保护影响评估表明，在没有保障、安全措施和减轻风险的机制的情况下，处理将导致自然人的权利和自由面临高风险，并且控制者认为，就可用的技术和实施成本而言，该风险无法通过合理手段减轻，则应当在开始处理活动之前咨询监管机构。此类高风险很可能由某些类型的处理以及处理的范围和频率引起，这也可能导致对自然人权利和自由的损害或干涉成为现实。监管机构应当在特定期限内对咨询请求作出答复。然而，监管机构在该期限内未作出反应不应影响监管机构根据本条例规定的任务和权力进行的任何干预，包括禁止处理操作的权力。作为该咨询过程的一部分，可以就所涉处理进行的数据保护影响评估的结果提交给监管机构，特别是为减轻对自然人权利和自由的风险而设想的措施。

(95) 处理者应当在必要时应控制者的请求，协助控制者确保遵守因开展数据保护影响评估和事先咨询监管机构而产生的义务。

(96) 在制定规定处理个人数据的立法或监管措施的过程中，也应当咨询监管机构，以确保预期处理符合本条例，特别是减轻数据主体所涉及的风险。

(97) 如果处理由公共机构进行，但法院或独立司法机构在行使其司法职能时除外；如果在私营部门，处理由控制者进行，而其核心活动包括需要对数据主体进行大规模定期和系统性监控的处理操作；或者如果控制者或处理者的核心活动包括大规模处理特殊类别的个人数据以及关于刑事定罪和犯罪的数据，则应当由一名在数据保护法律和实践方面具有专业知识的人员协助控制者或处理者监控内部对本条例的遵守情况。在私营部门，控制者的核心活动涉及其主要活动，而不涉及作为辅助活动的个人数据处理。必要的专业知识水平应当尤其根据所进行的个人数据处理操作来确定

and the protection required for the personal data processed by the controller or the processor. Such data protection officers, whether or not they are an employee of the controller, should be in a position to perform their duties and tasks in an independent manner.

(98) Associations or other bodies representing categories of controllers or processors should be encouraged to draw up codes of conduct, within the limits of this Regulation, so as to facilitate the effective application of this Regulation, taking account of the specific characteristics of the processing carried out in certain sectors and the specific needs of micro, small and medium enterprises. In particular, such codes of conduct could calibrate the obligations of controllers and processors, taking into account the risk likely to result from the processing for the rights and freedoms of natural persons.

(99) When drawing up a code of conduct, or when amending or extending such a code, associations and other bodies representing categories of controllers or processors should consult relevant stakeholders, including data subjects where feasible, and have regard to submissions received and views expressed in response to such consultations.

(100) In order to enhance transparency and compliance with this Regulation, the establishment of certification mechanisms and data protection seals and marks should be encouraged, allowing data subjects to quickly assess the level of data protection of relevant products and services.

(101) Flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation. The increase in such flows has raised new challenges and concerns with regard to the protection of personal data. However, when personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation. In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation. A transfer could take place only if, subject to the other provisions of this Regulation, the conditions laid down in the provisions of this Regulation relating to the transfer of personal data to third countries or international organisations are complied with by the controller or processor.

(102) This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subjects. Member States may conclude international agreements which involve the transfer of personal data to third countries or international organisations, as far as such agreements do not affect this Regulation or any other provisions of Union law and include an appropriate level of protection for the fundamental rights of the data subjects.

(103) The Commission may decide with effect for the entire Union that a third country, a territory or specified sector within a third country, or an international organisation, offers an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third country or international organisation which is considered to provide such level of protection. In such cases, transfers of personal data to that third country or international organisation may take place without the need to obtain any further authorisation. The Commission may also decide, having given notice and a full statement setting out the reasons to the third country or international organisation, to revoke such a decision.

(104) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of the third country, or of a territory or specified sector within a third country, take into account how a particular third country respects the rule of law, access to justice as well as international human rights norms and standards and its general and sectoral law, including legislation concerning public security, defence and national security as well as public order and criminal law. The adoption of an adequacy decision with regard to a territory or a specified sector in a third country should take into account clear and objective criteria, such as specific processing activities and the scope of applicable legal standards and legislation in force in the third country. The third country should offer guarantees ensuring an adequate level of

以及对控制者或处理者所处理个人数据所需的保护。此类数据保护官，无论是否为控制者的雇员，均应能够以独立的方式履行其职责和任务。

(98) 应当鼓励代表各类控制者或处理者的协会或其他机构在本条例范围内制定行为准则，以便利本条例的有效适用，同时考虑到某些行业所开展处理的特定特征以及微型、小型和中型企业的特定需求。特别是，此类行为准则可以调整控制者和处理者的义务，同时考虑到处理对自然人的权利和自由可能造成的风险。

(99) 在制定行为准则，或修订或扩展此类准则时，代表各类控制者或处理者的协会和其他机构应咨询相关利益相关方，包括在可行情况下咨询数据主体，并应考虑所收到的提交材料以及对此类咨询所表达的意见。

(100) 为增强透明度和对本条例的遵守，应鼓励建立认证机制以及数据保护印章和标记，使数据主体能够快速评估相关产品和服务的保护水平。

(101) 个人数据向欧盟以外国家及国际组织的流出与流入，对于扩展国际贸易和国际合作是必要的。此类流动的增加在个人数据保护方面带来了新的挑战和关切。然而，当个人数据从欧盟传输至第三国或国际组织的控制者、处理者或其他接收方时，本条例在欧盟内所确保的对自然人的保护水平不应受到损害，包括在个人数据从第三国或国际组织继续传输至同一或另一第三国或国际组织的控制者、处理者的情形下。在任何情况下，向第三国和国际组织的传输只能完全遵守本条例进行。只有在控制者或处理者遵守本条例中关于向第三国或国际组织传输个人数据的条款所规定的条件(且不违反本条例其他规定)的情况下，方可进行传输。

(102) 本条例不影响欧盟与第三国之间缔结的规范个人数据传输(包括对数据主体的适当保障措施)的国际协定。成员国可以缔结涉及向第三国或国际组织传输个人数据的国际协定，只要此类协定不影响本条例或欧盟法的任何其他条款，并包含对数据主体基本权利的适当保护水平。

(103) 委员会可以作出对全欧盟有效的决定，认定某一第三国、第三国内的某一领土或特定部门、或某一国际组织提供充分水平的数据保护，从而就该被视为提供此种保护水平的第三国或国际组织在全欧盟范围内提供法律确定性和统一性。在此类情形下，向该第三国或国际组织的个人数据传输无需获得任何进一步授权即可进行。委员会在通知该第三国或国际组织并充分说明理由后，也可决定撤销该决定。

(104) 根据欧盟所赖以建立的基本价值观，特别是对人权的保护，委员会在评估第三国或第三国内的某一领土或特定部门时，应当考虑该特定第三国如何尊重法治、司法救济途径以及国际人权规范和标准及其一般法和部门法，包括有关公共安全、国防和国家安全以及公共秩序和刑法的立法。就第三国内的某一领土或特定部门通过充分性认定时，应当考虑明确和客观的标准，例如具体的处理活动以及该第三国现行适用法律标准和立法的范围。该第三国应当提供保障，确保适当水平的

protection essentially equivalent to that ensured within the Union, in particular where personal data are processed in one or several specific sectors. In particular, the third country should ensure effective independent data protection supervision and should provide for cooperation mechanisms with the Member States' data protection authorities, and the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress.

(105) Apart from the international commitments the third country or international organisation has entered into, the Commission should take account of obligations arising from the third country's or international organisation's participation in multilateral or regional systems in particular in relation to the protection of personal data, as well as the implementation of such obligations. In particular, the third country's accession to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data and its Additional Protocol should be taken into account. The Commission should consult the Board when assessing the level of protection in third countries or international organisations.

(106) The Commission should monitor the functioning of decisions on the level of protection in a third country, a territory or specified sector within a third country, or an international organisation, and monitor the functioning of decisions adopted on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC. In its adequacy decisions, the Commission should provide for a periodic review mechanism of their functioning. That periodic review should be conducted in consultation with the third country or international organisation in question and take into account all relevant developments in the third country or international organisation. For the purposes of monitoring and of carrying out the periodic reviews, the Commission should take into consideration the views and findings of the European Parliament and of the Council as well as of other relevant bodies and sources. The Commission should evaluate, within a reasonable time, the functioning of the latter decisions and report any relevant findings to the Committee within the meaning of Regulation (EU) No 182/2011 of the European Parliament and of the Council ([1]) as established under this Regulation, to the European Parliament and to the Council.

(107) The Commission may recognise that a third country, a territory or a specified sector within a third country, or an international organisation no longer ensures an adequate level of data protection. Consequently the transfer of personal data to that third country or international organisation should be prohibited, unless the requirements in this Regulation relating to transfers subject to appropriate safeguards, including binding corporate rules, and derogations for specific situations are fulfilled. In that case, provision should be made for consultations between the Commission and such third countries or international organisations. The Commission should, in a timely manner, inform the third country or international organisation of the reasons and enter into consultations with it in order to remedy the situation.

(108) In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or contractual clauses authorised by a supervisory authority. Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union, including the availability of enforceable data subject rights and of effective legal remedies, including to obtain effective administrative or judicial redress and to claim compensation, in the Union or in a third country. They should relate in particular to compliance with the general principles relating to personal data processing, the principles of data protection by design and by default. Transfers may also be carried out by public authorities or bodies with public authorities or bodies in third countries or with international organisations with corresponding duties or functions, including on the basis of provisions to be inserted into administrative arrangements, such as a memorandum of understanding, providing for enforceable and effective rights for data subjects. Authorisation by the competent supervisory authority should be obtained when the safeguards are provided for in administrative arrangements that are not legally binding.

(109) The possibility for the controller or processor to use standard data-protection clauses adopted by the Commission or by a supervisory authority should prevent controllers or processors neither from including the

([1]) Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

基本上等同于联盟内所确保的保护，特别是在一个或多个特定部门处理个人数据的情况下。特别是，第三国应确保有效的独立数据保护监督，并应规定与成员国数据保护机构的合作机制，且应向数据主体提供有效且可执行的权利以及有效的行政和司法救济。

(105) 除第三国或国际组织已加入的国际承诺外，委员会还应考虑第三国或国际组织参与多边或区域体系所产生的义务，特别是与个人数据保护相关的义务，以及此类义务的履行情况。尤其应考虑第三国加入1981年1月28日《欧洲委员会关于在个人数据自动处理方面保护个人的公约》及其附加议定书的情况。委员会在评估第三国或国际组织的保护水平时应咨询委员会。

(106) 委员会应监督关于第三国、第三国境内特定领土或特定部门或国际组织保护水平的决定的运作情况，并监督根据指令95/46/EC第25(6)条或第26(4)条通过的决定的运作情况。在其充分性认定中，委员会应规定对其运作情况进行定期审查的机制。该定期审查应与相关第三国或国际组织协商进行，并考虑第三国或国际组织中的所有相关发展。为监督和开展定期审查之目的，委员会应考虑欧洲议会和理事会以及其他相关机构和来源的意见和结论。委员会应在合理时间内评估后述决定的运作情况，并向根据本条例设立的欧洲议会和理事会条例(EU) No 182/2011(1)含义内的委员会、欧洲议会和理事会报告任何相关结论。

(107) 委员会可认定第三国、第三国境内某一领土或特定部门或国际组织不再确保充分的数据保护水平。因此，应向该第三国或国际组织传输个人数据的行为应被禁止，除非满足本条例中关于受适当保障措施约束的传输(包括有约束力的公司规则)以及特定情形下的克减的要求。在此情况下，应规定委员会与此类第三国或国际组织之间的协商。委员会应及时将理由告知该第三国或国际组织，并与其进行协商以补救该情况。

(108) 在无充分性认定的情况下，控制者或处理者应采取措施，通过为数据主体提供适当保障措施来弥补第三国数据保护的缺失。此类适当保障措施可包括使用有约束力的公司规则、委员会通过的标准数据保护条款、监管机构通过的标准数据保护条款或监管机构授权的合同条款。这些保障措施应确保遵守与联盟内处理相适应的数据保护要求和数据主体的权利，包括在联盟内或第三国可获得可强制执行的数据主体权利和有效的法律救济，包括获得有效的行政或司法救济以及索赔。它们应特别涉及遵守与个人数据处理相关的一般原则、数据保护设计和默认数据保护原则。传输也可由公共当局或机构与第三国具有相应职责或职能的公共当局或机构或国际组织进行，包括依据将纳入行政安排(如谅解备忘录)的条款进行，为数据主体提供可强制执行的有效权利。当保障措施规定在不具有法律约束力的行政安排中时，应获得主管监管机构的授权。

(109) 控制者或处理者使用委员会或监管机构通过的标准数据保护条款的可能性，既不应阻止控制者或处理者纳入

(1) 欧洲议会和理事会2011年2月16日第(EU) No 182/2011号条例，规定有关成员国对委员会行使实施权力进行控制机制的规则和一般原则(OJ L 55, 28.2.2011, p.13)。

standard data-protection clauses in a wider contract, such as a contract between the processor and another processor, nor from adding other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects. Controllers and processors should be encouraged to provide additional safeguards via contractual commitments that supplement standard protection clauses.

(110) A group of undertakings, or a group of enterprises engaged in a joint economic activity, should be able to make use of approved binding corporate rules for its international transfers from the Union to organisations within the same group of undertakings, or group of enterprises engaged in a joint economic activity, provided that such corporate rules include all essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data.

(111) Provisions should be made for the possibility for transfers in certain circumstances where the data subject has given his or her explicit consent, where the transfer is occasional and necessary in relation to a contract or a legal claim, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies. Provision should also be made for the possibility for transfers where important grounds of public interest laid down by Union or Member State law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In the latter case, such a transfer should not involve the entirety of the personal data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or, if they are to be the recipients, taking into full account the interests and fundamental rights of the data subject.

(112) Those derogations should in particular apply to data transfers required and necessary for important reasons of public interest, for example in cases of international data exchange between competition authorities, tax or customs administrations, between financial supervisory authorities, between services competent for social security matters, or for public health, for example in the case of contact tracing for contagious diseases or in order to reduce and/or eliminate doping in sport. A transfer of personal data should also be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's or another person's vital interests, including physical integrity or life, if the data subject is incapable of giving consent. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of data to a third country or an international organisation. Member States should notify such provisions to the Commission. Any transfer to an international humanitarian organisation of personal data of a data subject who is physically or legally incapable of giving consent, with a view to accomplishing a task incumbent under the Geneva Conventions or to complying with international humanitarian law applicable in armed conflicts, could be considered to be necessary for an important reason of public interest or because it is in the vital interest of the data subject.

(113) Transfers which can be qualified as not repetitive and that only concern a limited number of data subjects, could also be possible for the purposes of the compelling legitimate interests pursued by the controller, when those interests are not overridden by the interests or rights and freedoms of the data subject and when the controller has assessed all the circumstances surrounding the data transfer. The controller should give particular consideration to the nature of the personal data, the purpose and duration of the proposed processing operation or operations, as well as the situation in the country of origin, the third country and the country of final destination, and should provide suitable safeguards to protect fundamental rights and freedoms of natural persons with regard to the processing of their personal data. Such transfers should be possible only in residual cases where none of the other grounds for transfer are applicable. For scientific or historical research purposes or statistical purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration. The controller should inform the supervisory authority and the data subject about the transfer.

(114) In any case, where the Commission has taken no decision on the adequate level of data protection in a third country, the controller or processor should make use of solutions that provide data subjects with enforceable and effective rights as regards the processing of their data in the Union once those data have been transferred so that that they will continue to benefit from fundamental rights and safeguards.

更广泛合同(例如处理者与另一处理者之间的合同)中的标准数据保护条款，也不得添加其他条款或附加保障措施，前提是它们不直接或间接与委员会或监管机构通过的标准合同条款相抵触，或不损害数据主体的基本权利或自由。应鼓励控制者和处理者通过补充标准保护条款的合同承诺提供附加保障措施。

(110) 企业集团或从事联合经济活动的企业集团，应能够利用经批准的有约束力的公司规则，将其从联盟向同一企业集团或从事联合经济活动的企业集团内的组织进行国际传输，前提是此类公司规则包含所有基本原则和可执行权利，以确保对个人数据传输或传输类别提供适当保障。

(111) 应当规定在特定情形下可以进行传输的可能性，包括数据主体已给予其明确同意的情形，传输是偶尔发生的且就合同或法律主张而言是必要的情形，无论该主张是在司法程序中还是在行政程序或任何庭外程序中提出，包括向监管机构提出的程序。还应当规定在欧盟或成员国法律规定的公共利益重要理由有此要求时，或者传输是从依法设立且供公众或具有正当利益的人查阅的登记册中作出时，可以进行传输的可能性。在后一种情形下，此类传输不应涉及登记册中所含个人数据的全部或全部类别的数据；并且，当登记册供具有正当利益的人查阅时，传输应当仅应这些人的请求作出，或者如果这些人将成为接收方，则应充分考虑数据主体的利益和基本权利。

(112) 这些例外尤其应当适用于因公共利益重要原因而要求且必要的个人数据传输，例如在竞争主管机构之间、税务或海关管理部门之间、金融监管机构之间、负责社会保障事务的机构之间进行国际数据交换的情形，或出于公共卫生目的的情形，例如为追踪传染病接触者或为减少和/或消除体育运动中的兴奋剂而进行的情形。当为了保护对数据主体或他人的重大利益(包括身体完整性或生命)至关重要的利益而必要时，如果数据主体无法给予同意，个人数据的传输也应当被视为合法。在没有充分性认定的情况下，欧盟或成员国法律可以出于公共利益的重要原因，明确限制特定类别的数据传输至第三国或国际组织。成员国应当将此规定通知委员会。向国际人道主义组织传输身体上或法律上无法给予同意的数据主体的个人数据，以完成为《日内瓦公约》所规定的任务或遵守适用于武装冲突的国际人道主义法，可被视为出于公共利益的重要原因或因为符合数据主体的重大利益而必要。

(113) 可被定性为非重复性且仅涉及有限数量数据主体的传输，在控制者所追求的紧迫正当利益有此需要时也可以进行，前提是这些利益不被数据主体的利益或权利和自由所压倒，且控制者已评估与数据传输相关的所有情况。控制者应当特别考虑个人数据的性质、拟议处理操作的目的和持续时间，以及来源国、第三国和最终目的地国的情况，并应当提供适当保障措施，以保护自然人在其个人数据处理方面的基本权利和自由。此类传输应当仅在剩余情形下、即其他传输依据均不适用时才可进行。为科学或历史研究目的或统计目的，应当考虑社会对增加知识的正当期望。控制者应当将传输事宜告知监管机构和数据主体。

(114) 在任何情况下，如果委员会尚未就第三国的充分数据保护水平作出决定，控制者或处理者应采用能够为数据主体在其数据被传输后在联盟内处理其数据方面提供可执行和有效权利的解决方案，使其继续享有基本权利和保障。

(115) Some third countries adopt laws, regulations and other legal acts which purport to directly regulate the processing activities of natural and legal persons under the jurisdiction of the Member States. This may include judgments of courts or tribunals or decisions of administrative authorities in third countries requiring a controller or processor to transfer or disclose personal data, and which are not based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State. The extraterritorial application of those laws, regulations and other legal acts may be in breach of international law and may impede the attainment of the protection of natural persons ensured in the Union by this Regulation. Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met. This may be the case, inter alia, where disclosure is necessary for an important ground of public interest recognised in Union or Member State law to which the controller is subject.

(116) When personal data moves across borders outside the Union it may put at increased risk the ability of natural persons to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints. Therefore, there is a need to promote closer cooperation among data protection supervisory authorities to help them exchange information and carry out investigations with their international counterparts. For the purposes of developing international cooperation mechanisms to facilitate and provide international mutual assistance for the enforcement of legislation for the protection of personal data, the Commission and the supervisory authorities should exchange information and cooperate in activities related to the exercise of their powers with competent authorities in third countries, based on reciprocity and in accordance with this Regulation.

(117) The establishment of supervisory authorities in Member States, empowered to perform their tasks and exercise their powers with complete independence, is an essential component of the protection of natural persons with regard to the processing of their personal data. Member States should be able to establish more than one supervisory authority, to reflect their constitutional, organisational and administrative structure.

(118) The independence of supervisory authorities should not mean that the supervisory authorities cannot be subject to control or monitoring mechanisms regarding their financial expenditure or to judicial review.

(119) Where a Member State establishes several supervisory authorities, it should establish by law mechanisms for ensuring the effective participation of those supervisory authorities in the consistency mechanism. That Member State should in particular designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the mechanism, to ensure swift and smooth cooperation with other supervisory authorities, the Board and the Commission.

(120) Each supervisory authority should be provided with the financial and human resources, premises and infrastructure necessary for the effective performance of their tasks, including those related to mutual assistance and cooperation with other supervisory authorities throughout the Union. Each supervisory authority should have a separate, public annual budget, which may be part of the overall state or national budget.

(121) The general conditions for the member or members of the supervisory authority should be laid down by law in each Member State and should in particular provide that those members are to be appointed, by means of a transparent procedure, either by the parliament, government or the head of State of the Member State on the basis of a proposal from the government, a member of the government, the parliament or a chamber of the parliament, or by an independent body entrusted under Member State law. In order to ensure the independence of the supervisory authority, the member or members should act with integrity, refrain from any action that is incompatible with their duties and should not, during their term of office, engage in any incompatible occupation, whether gainful or not. The supervisory authority should have its own staff, chosen by the supervisory authority or an independent body established by Member State law, which should be subject to the exclusive direction of the member or members of the supervisory authority.

(122) Each supervisory authority should be competent on the territory of its own Member State to exercise the powers and to perform the tasks conferred on it in accordance with this Regulation. This should cover in particular the

(115) 一些第三国通过法律、法规和其他法律行为，意图直接规范成员国管辖下的自然人和法人的处理活动。这可能包括第三国法院或法庭的判决或行政机关的决定，要求控制者或处理者传输或披露个人数据，且这些判决或决定并非基于请求第三国与欧盟或成员国之间生效的国际协定，例如司法协助条约。这些法律、法规和其他法律行为的域外适用可能违反国际法，并可能妨碍本条例在欧盟所确保的对自然人的保护之实现。只有在符合本条例关于向第三国传输的条件时，才应当允许传输。除其他情形外，当披露对于控制者所受约束的欧盟或成员国法律所承认的公共利益重要理由而言是必要时，即可能属于此种情形。

(116) 当个人数据跨境传输至欧盟以外时，可能会增加自然人行使数据保护权利的能力所受的风险，尤其是保护自身免受该信息非法使用或披露的能力。与此同时，监管机构可能会发现其无法就境外活动处理投诉或开展调查。其在跨境背景下开展合作的努力也可能因预防性或补救性权力不足、法律制度不一致以及资源限制等实际障碍而受到阻碍。因此，有必要促进数据保护监管机构之间更紧密的合作，以帮助其与国际同行交换信息并开展调查。为发展国际合作机制以促进并为个人数据保护立法的执行提供国际互助，委员会和监管机构应当基于互惠并依照本条例，与第三国主管机构交换信息并在与其行使权力相关的活动中开展合作。

(117) 在成员国设立监管机构，授权其完全独立地履行任务和行使权力，是保护自然人在其个人数据处理方面的一项基本组成部分。成员国应能够设立一个以上的监管机构，以反映其宪法、组织和行政结构。

(118) 监管机构的独立性不应意味着监管机构不能就其财政支出接受控制或监督机制或司法审查。

(119) 当一成员国设立多个监管机构时，应通过法律确立机制，确保这些监管机构有效参与一致性机制。该成员国尤其应指定一个监管机构作为单一联络点，以便这些机构有效参与该机制，确保与其他监管机构、委员会和欧盟委员会迅速顺畅合作。

(120) 每个监管机构应获得有效履行其任务所必需的财政和人力资源、场所和基础设施，包括与整个联盟内其他监管机构相互协助和合作相关的任务。每个监管机构应拥有单独的公开年度预算，该预算可以是整体国家或国民预算的一部分。

(121) 监管机构成员的一般条件应由各成员国法律予以规定，并尤其应规定，这些成员应通过透明程序任命，或由成员国议会、政府或国家元首根据政府、政府成员、议会或议会一院的提议任命，或由根据成员国法律委托的独立机构任命。为确保监管机构的独立性，该成员或成员们应诚信行事，避免任何与其职责不符的行为，并且在其任期内不得从事任何不相容的职业，无论是否有报酬。监管机构应拥有自己的工作人员，由监管机构或根据成员国法律设立的独立机构选定，这些工作人员应仅接受监管机构成员或成员们的指导。

(122) 每个监管机构应在其本国成员国领土内有权行使本条例赋予的权力并履行本条例赋予的任务。这尤其应涵盖

processing in the context of the activities of an establishment of the controller or processor on the territory of its own Member State, the processing of personal data carried out by public authorities or private bodies acting in the public interest, processing affecting data subjects on its territory or processing carried out by a controller or processor not established in the Union when targeting data subjects residing on its territory. This should include handling complaints lodged by a data subject, conducting investigations on the application of this Regulation and promoting public awareness of the risks, rules, safeguards and rights in relation to the processing of personal data.

(123) The supervisory authorities should monitor the application of the provisions pursuant to this Regulation and contribute to its consistent application throughout the Union, in order to protect natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the internal market. For that purpose, the supervisory authorities should cooperate with each other and with the Commission, without the need for any agreement between Member States on the provision of mutual assistance or on such cooperation.

(124) Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union and the controller or processor is established in more than one Member State, or where processing taking place in the context of the activities of a single establishment of a controller or processor in the Union substantially affects or is likely to substantially affect data subjects in more than one Member State, the supervisory authority for the main establishment of the controller or processor or for the single establishment of the controller or processor should act as lead authority. It should cooperate with the other authorities concerned, because the controller or processor has an establishment on the territory of their Member State, because data subjects residing on their territory are substantially affected, or because a complaint has been lodged with them. Also where a data subject not residing in that Member State has lodged a complaint, the supervisory authority with which such complaint has been lodged should also be a supervisory authority concerned. Within its tasks to issue guidelines on any question covering the application of this Regulation, the Board should be able to issue guidelines in particular on the criteria to be taken into account in order to ascertain whether the processing in question substantially affects data subjects in more than one Member State and on what constitutes a relevant and reasoned objection.

(125) The lead authority should be competent to adopt binding decisions regarding measures applying the powers conferred on it in accordance with this Regulation. In its capacity as lead authority, the supervisory authority should closely involve and coordinate the supervisory authorities concerned in the decision-making process. Where the decision is to reject the complaint by the data subject in whole or in part, that decision should be adopted by the supervisory authority with which the complaint has been lodged.

(126) The decision should be agreed jointly by the lead supervisory authority and the supervisory authorities concerned and should be directed towards the main or single establishment of the controller or processor and be binding on the controller and processor. The controller or processor should take the necessary measures to ensure compliance with this Regulation and the implementation of the decision notified by the lead supervisory authority to the main establishment of the controller or processor as regards the processing activities in the Union.

(127) Each supervisory authority not acting as the lead supervisory authority should be competent to handle local cases where the controller or processor is established in more than one Member State, but the subject matter of the specific processing concerns only processing carried out in a single Member State and involves only data subjects in that single Member State, for example, where the subject matter concerns the processing of employees' personal data in the specific employment context of a Member State. In such cases, the supervisory authority should inform the lead supervisory authority without delay about the matter. After being informed, the lead supervisory authority should decide, whether it will handle the case pursuant to the provision on cooperation between the lead supervisory authority and other supervisory authorities concerned ('one-stop-shop mechanism'), or whether the supervisory authority which informed it should handle the case at local level. When deciding whether it will handle the case, the lead supervisory authority should take into account whether there is an establishment of the controller or processor in the Member State of the supervisory authority which informed it in order to ensure effective enforcement of a decision *vis-à-vis* the controller or processor. Where the lead supervisory authority decides to handle the case, the supervisory authority which informed it should have the

在控制者或处理者在其本国成员国境内的机构活动背景下的处理、公共当局或为公共利益行事的私人机构进行的个人数据处理、影响其境内数据主体的处理，或由未在欧盟设立的控制者或处理者针对居住在其境内的数据主体进行的处理。这应包括处理数据主体提出的投诉、就本条例的适用进行调查，以及促进公众对个人数据处理相关风险、规则、保障措施和权利的认识。

(123) 监管机构应监督本条例各项规定的适用，并促进其在整个欧盟的一致适用，以在个人数据处理方面保护自然人，并促进个人数据在内部市场内的自由流动。为此目的，监管机构应相互合作并与欧盟委员会合作，无需成员国之间就提供互助或此类合作达成任何协议。

(124) 当个人数据处理发生在控制者或处理者在欧盟的机构活动背景下，且该控制者或处理者在多个成员国设有机构，或者当处理发生在控制者或处理者在欧盟的单一机构活动背景下并实质影响或可能实质影响多个成员国的数据主体时，控制者或处理者主要机构或单一机构所在的监管机构应作为牵头监管机构。它应与其他相关机构合作，因为控制者或处理者在其成员国境内设有机构，因为居住在其境内的数据主体受到实质影响，或因为已向其提出投诉。此外，如果非居住在该成员国的数据主体提出投诉，收到该投诉的监管机构也应成为相关监管机构。在发布关于本条例适用任何问题的指南的任务范围内，委员会应能够特别就为确定有关处理是否实质影响多个成员国的数据主体而应考虑的标准，以及什么构成相关且有理由的反对意见发布指南。

(125) 主导监管机构应有权就依据本条例行使其被授予权力的措施通过具有约束力的决定。作为主导监管机构，监管机构应在决策过程中密切让相关监管机构参与并与之协调。如果决定全部或部分驳回数据主体的投诉，该决定应由受理投诉的监管机构通过。

(126) 该决定应由主导监管机构与相关监管机构共同商定，并应针对控制者或处理者的主要或单一营业场所，且对控制者和处理者具有约束力。控制者或处理者应采取必要措施，确保遵守本条例，并执行主导监管机构就联盟内的处理活动通知控制者或处理者主要营业场所的决定。

(127) 不担任主导监管机构的每一监管机构，应当有权处理控制者或处理者设立在多个成员国、但特定处理事项仅涉及在单一成员国进行的处理且仅涉及该单一成员国数据主体的本地案件，例如，该事项涉及在某一成员国的特定雇佣背景下处理雇员的个人数据。在此类情形下，该监管机构应当毫不迟延地将该事项告知主导监管机构。在被告知后，主导监管机构应当决定，其将依据关于主导监管机构与其他相关监管机构之间合作的条款("一站式机制")处理该案件，还是由告知它的监管机构在本地层面处理该案件。在决定是否处理该案件时，主导监管机构应当考虑控制者或处理者是否在告知它的监管机构所属成员国设有机构，以确保针对控制者或处理者的决定得到有效执行。主导监管机构决定处理该案件的，告知它的监管机构应当具有

possibility to submit a draft for a decision, of which the lead supervisory authority should take utmost account when preparing its draft decision in that one-stop-shop mechanism.

(128) The rules on the lead supervisory authority and the one-stop-shop mechanism should not apply where the processing is carried out by public authorities or private bodies in the public interest. In such cases the only supervisory authority competent to exercise the powers conferred to it in accordance with this Regulation should be the supervisory authority of the Member State where the public authority or private body is established.

(129) In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have in each Member State the same tasks and effective powers, including powers of investigation, corrective powers and sanctions, and authorisation and advisory powers, in particular in cases of complaints from natural persons, and without prejudice to the powers of prosecutorial authorities under Member State law, to bring infringements of this Regulation to the attention of the judicial authorities and engage in legal proceedings. Such powers should also include the power to impose a temporary or definitive limitation, including a ban, on processing. Member States may specify other tasks related to the protection of personal data under this Regulation. The powers of supervisory authorities should be exercised in accordance with appropriate procedural safeguards set out in Union and Member State law, impartially, fairly and within a reasonable time. In particular each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case, respect the right of every person to be heard before any individual measure which would affect him or her adversely is taken and avoid superfluous costs and excessive inconveniences for the persons concerned. Investigatory powers as regards access to premises should be exercised in accordance with specific requirements in Member State procedural law, such as the requirement to obtain a prior judicial authorisation. Each legally binding measure of the supervisory authority should be in writing, be clear and unambiguous, indicate the supervisory authority which has issued the measure, the date of issue of the measure, bear the signature of the head, or a member of the supervisory authority authorised by him or her, give the reasons for the measure, and refer to the right of an effective remedy. This should not preclude additional requirements pursuant to Member State procedural law. The adoption of a legally binding decision implies that it may give rise to judicial review in the Member State of the supervisory authority that adopted the decision.

(130) Where the supervisory authority with which the complaint has been lodged is not the lead supervisory authority, the lead supervisory authority should closely cooperate with the supervisory authority with which the complaint has been lodged in accordance with the provisions on cooperation and consistency laid down in this Regulation. In such cases, the lead supervisory authority should, when taking measures intended to produce legal effects, including the imposition of administrative fines, take utmost account of the view of the supervisory authority with which the complaint has been lodged and which should remain competent to carry out any investigation on the territory of its own Member State in liaison with the competent supervisory authority.

(131) Where another supervisory authority should act as a lead supervisory authority for the processing activities of the controller or processor but the concrete subject matter of a complaint or the possible infringement concerns only processing activities of the controller or processor in the Member State where the complaint has been lodged or the possible infringement detected and the matter does not substantially affect or is not likely to substantially affect data subjects in other Member States, the supervisory authority receiving a complaint or detecting or being informed otherwise of situations that entail possible infringements of this Regulation should seek an amicable settlement with the controller and, if this proves unsuccessful, exercise its full range of powers. This should include: specific processing carried out in the territory of the Member State of the supervisory authority or with regard to data subjects on the territory of that Member State; processing that is carried out in the context of an offer of goods or services specifically aimed at data subjects in the territory of the Member State of the supervisory authority; or processing that has to be assessed taking into account relevant legal obligations under Member State law.

(132) Awareness-raising activities by supervisory authorities addressed to the public should include specific measures directed at controllers and processors, including micro, small and medium-sized enterprises, as well as natural persons in particular in the educational context.

提交决定草案的可能性，主导监管机构在该一站式机制中编制其决定草案时应尽可能考虑该草案。

(128) 关于主导监管机构和一站式机制的规则不适用于公共当局或私人机构为公共利益进行的处理。在此类情况下，唯一有权行使本条例赋予权力的监管机构应是公共当局或私人机构设立所在成员国的监管机构。

(129) 为确保本条例在整个联盟内得到一致监督和执行，各成员国的监管机构应具有相同的任务和有效权力，包括调查权、纠正权和制裁权，以及授权和咨询权，特别是在自然人投诉的情况下，并在不影响成员国法律下检察机关权力的情况下，将违反本条例的行为提请司法机关注意并参与法律程序。此类权力还应包括对处理施加临时或最终限制(包括禁令)的权力。成员国可规定与本条例下个人数据保护相关的其他任务。监管机构的权力应依照联盟和成员国法律规定的适当程序保障，公正、公平并在合理时间内行使。特别是，每项措施应适当、必要且相称，以确保遵守本条例，同时考虑每个个案的情况，尊重每个人在任何可能对其产生不利影响的个别措施采取之前发表意见的权利，并避免给相关个人造成多余成本和过度不便。关于进入场所的调查权应依照成员国程序法中的具体要求行使，例如获得事先司法授权的要求。监管机构的每项具有法律约束力的措施应以书面形式作出，清晰明确，指明发布该措施的监管机构、措施的发布日期，由负责人或经其授权的监管机构成员签名，说明措施的理由，并提及获得有效救济的权利。这不应排除成员国程序法下的额外要求。通过具有法律约束力的决定意味着该决定可能在通过该决定的监管机构所在成员国引起司法审查。

(130) 如果受理投诉的监管机构不是主导监管机构，主导监管机构应依照本条例规定的合作与一致性条款，与受理投诉的监管机构密切合作。在此类情况下，主导监管机构在采取旨在产生法律效力的措施(包括施加行政罚款)时，应尽可能考虑受理投诉的监管机构的意见，该监管机构应保留与其主管监管机构联络在其本国成员国领土上进行任何调查的权力。

(131) 当另一监管机构应当作为控制者或处理者处理活动的主导监管机构，但投诉的具体标的或可能的侵权行为仅涉及控制者或处理者在提出投诉或发现可能侵权行为的成员国内的处理活动，且该事项不实质影响或不太可能实质影响其他成员国的数据主体时，收到投诉或发现或以其他方式获悉存在可能违反本条例情形的监管机构应当寻求与控制者友好解决，如果证明不成功，则应行使其全部权力。这应包括：在监管机构所在成员国境内或针对该成员国境内数据主体进行的特定处理；在专门针对监管机构所在成员国境内数据主体的商品或服务提供背景下进行的处理；或必须考虑成员国法律下的相关法律义务进行评估的处理。

(132) 监管机构面向公众的提高认识活动应包括针对控制者和处理者(包括微型、小型和中型企业)以及自然人的具体措施，特别是在教育背景下。

(133) The supervisory authorities should assist each other in performing their tasks and provide mutual assistance, so as to ensure the consistent application and enforcement of this Regulation in the internal market. A supervisory authority requesting mutual assistance may adopt a provisional measure if it receives no response to a request for mutual assistance within one month of the receipt of that request by the other supervisory authority.

(134) Each supervisory authority should, where appropriate, participate in joint operations with other supervisory authorities. The requested supervisory authority should be obliged to respond to the request within a specified time period.

(135) In order to ensure the consistent application of this Regulation throughout the Union, a consistency mechanism for cooperation between the supervisory authorities should be established. That mechanism should in particular apply where a supervisory authority intends to adopt a measure intended to produce legal effects as regards processing operations which substantially affect a significant number of data subjects in several Member States. It should also apply where any supervisory authority concerned or the Commission requests that such matter should be handled in the consistency mechanism. That mechanism should be without prejudice to any measures that the Commission may take in the exercise of its powers under the Treaties.

(136) In applying the consistency mechanism, the Board should, within a determined period of time, issue an opinion, if a majority of its members so decides or if so requested by any supervisory authority concerned or the Commission. The Board should also be empowered to adopt legally binding decisions where there are disputes between supervisory authorities. For that purpose, it should issue, in principle by a two-thirds majority of its members, legally binding decisions in clearly specified cases where there are conflicting views among supervisory authorities, in particular in the cooperation mechanism between the lead supervisory authority and supervisory authorities concerned on the merits of the case, in particular whether there is an infringement of this Regulation.

(137) There may be an urgent need to act in order to protect the rights and freedoms of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded. A supervisory authority should therefore be able to adopt duly justified provisional measures on its territory with a specified period of validity which should not exceed three months.

(138) The application of such mechanism should be a condition for the lawfulness of a measure intended to produce legal effects by a supervisory authority in those cases where its application is mandatory. In other cases of cross-border relevance, the cooperation mechanism between the lead supervisory authority and supervisory authorities concerned should be applied and mutual assistance and joint operations might be carried out between the supervisory authorities concerned on a bilateral or multilateral basis without triggering the consistency mechanism.

(139) In order to promote the consistent application of this Regulation, the Board should be set up as an independent body of the Union. To fulfil its objectives, the Board should have legal personality. The Board should be represented by its Chair. It should replace the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data established by Directive 95/46/EC. It should consist of the head of a supervisory authority of each Member State and the European Data Protection Supervisor or their respective representatives. The Commission should participate in the Board's activities without voting rights and the European Data Protection Supervisor should have specific voting rights. The Board should contribute to the consistent application of this Regulation throughout the Union, including by advising the Commission, in particular on the level of protection in third countries or international organisations, and promoting cooperation of the supervisory authorities throughout the Union. The Board should act independently when performing its tasks.

(140) The Board should be assisted by a secretariat provided by the European Data Protection Supervisor. The staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation should perform its tasks exclusively under the instructions of, and report to, the Chair of the Board.

(141) Every data subject should have the right to lodge a complaint with a single supervisory authority, in particular in the Member State of his or her habitual residence, and the right to an effective judicial remedy in accordance

(133) 监管机构应相互协助履行其任务并提供相互协助，以确保本条例在内部市场的一致适用和执行。请求相互协助的监管机构，如果在另一监管机构收到该请求后一个月内未收到对相互协助请求的答复，可采取临时措施。

(134) 各监管机构应当酌情与其他监管机构参与联合行动。被请求的监管机构应当有义务在指定期限内对请求作出回应。

(135) 为确保本条例在整个联盟内的一致适用，应建立监管机构之间合作的一致性机制。该机制尤其应适用于监管机构打算采取旨在对处理操作产生法律效力的措施，而该处理操作实质影响多个成员国的大量数据主体的情形。该机制还应适用于任何相关监管机构或委员会请求此类事项应在一致性机制中处理的情形。该机制不应影响委员会根据条约行使其权力可能采取的任何措施。

(136) 在适用一致性机制时，如果其成员以多数票如此决定，或任何相关监管机构或委员会如此请求，董事会应在确定的时间内发表意见。董事会还应有权在监管机构之间存在争议时通过具有法律约束力的决定。为此，董事会应原则上以其成员的三分之二多数，在监管机构之间存在分歧的明确特定情形下通过具有法律约束力的决定，尤其是在主导监管机构与相关监管机构之间关于案件实质的合作机制中，特别是关于是否存在违反本条例的情形。

(137) 可能存在迫切需要采取行动以保护数据主体的权利和自由的情况，特别是当存在数据主体权利的执行可能受到严重阻碍的危险时。因此，监管机构应能够在其领土内采取有正当理由的临时措施，并规定不超过三个月的有效期。

(138) 在此类机制的适用为强制性的情形下，该机制的适用应成为监管机构旨在产生法律效力的措施合法性的条件。在其他具有跨境相关性的情形中，应适用主导监管机构与相关监管机构之间的合作机制，相关监管机构之间可在双边或多边基础上开展互助和联合行动，而无需触发一致性机制。

(139) 为促进本条例的一致适用，应设立董事会作为联盟的独立机构。为实现其目标，董事会应具有法律人格。董事会应由其主席代表。董事会应取代根据 Directive 95/46/EC 设立的个人数据处理保护工作组。董事会应由每个成员国的监管机构负责人和欧洲数据保护监督员或其各自的代表组成。委员会应参与董事会的活动但无表决权，欧洲数据保护监督员应拥有特定的表决权。董事会应促进本条例在整个联盟内的一致适用，包括向委员会提供建议，特别是关于第三国或国际组织的保护水平，并促进整个联盟内监管机构的合作。董事会在履行其任务时应独立行事。

(140) 委员会应由欧洲数据保护监督员提供的秘书处协助。参与执行本条例赋予委员会任务的欧洲数据保护监督员工作人员应完全按照委员会主席的指示执行其任务，并向委员会主席报告。

(141) 每个数据主体应当有权向单一监管机构提出投诉，特别是在其惯常居所所在的成员国，并有权根据以下规定获得有效的司法救济

with Article 47 of the Charter if the data subject considers that his or her rights under this Regulation are infringed or where the supervisory authority does not act on a complaint, partially or wholly rejects or dismisses a complaint or does not act where such action is necessary to protect the rights of the data subject. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be given to the data subject. In order to facilitate the submission of complaints, each supervisory authority should take measures such as providing a complaint submission form which can also be completed electronically, without excluding other means of communication.

(142) Where a data subject considers that his or her rights under this Regulation are infringed, he or she should have the right to mandate a not-for-profit body, organisation or association which is constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest and is active in the field of the protection of personal data to lodge a complaint on his or her behalf with a supervisory authority, exercise the right to a judicial remedy on behalf of data subjects or, if provided for in Member State law, exercise the right to receive compensation on behalf of data subjects. A Member State may provide for such a body, organisation or association to have the right to lodge a complaint in that Member State, independently of a data subject's mandate, and the right to an effective judicial remedy where it has reasons to consider that the rights of a data subject have been infringed as a result of the processing of personal data which infringes this Regulation. That body, organisation or association may not be allowed to claim compensation on a data subject's behalf independently of the data subject's mandate.

(143) Any natural or legal person has the right to bring an action for annulment of decisions of the Board before the Court of Justice under the conditions provided for in Article 263 TFEU. As addressees of such decisions, the supervisory authorities concerned which wish to challenge them have to bring action within two months of being notified of them, in accordance with Article 263 TFEU. Where decisions of the Board are of direct and individual concern to a controller, processor or complainant, the latter may bring an action for annulment against those decisions within two months of their publication on the website of the Board, in accordance with Article 263 TFEU. Without prejudice to this right under Article 263 TFEU, each natural or legal person should have an effective judicial remedy before the competent national court against a decision of a supervisory authority which produces legal effects concerning that person. Such a decision concerns in particular the exercise of investigative, corrective and authorisation powers by the supervisory authority or the dismissal or rejection of complaints. However, the right to an effective judicial remedy does not encompass measures taken by supervisory authorities which are not legally binding, such as opinions issued by or advice provided by the supervisory authority. Proceedings against a supervisory authority should be brought before the courts of the Member State where the supervisory authority is established and should be conducted in accordance with that Member State's procedural law. Those courts should exercise full jurisdiction, which should include jurisdiction to examine all questions of fact and law relevant to the dispute before them.

Where a complaint has been rejected or dismissed by a supervisory authority, the complainant may bring proceedings before the courts in the same Member State. In the context of judicial remedies relating to the application of this Regulation, national courts which consider a decision on the question necessary to enable them to give judgment, may, or in the case provided for in Article 267 TFEU, must, request the Court of Justice to give a preliminary ruling on the interpretation of Union law, including this Regulation. Furthermore, where a decision of a supervisory authority implementing a decision of the Board is challenged before a national court and the validity of the decision of the Board is at issue, that national court does not have the power to declare the Board's decision invalid but must refer the question of validity to the Court of Justice in accordance with Article 267 TFEU as interpreted by the Court of Justice, where it considers the decision invalid. However, a national court may not refer a question on the validity of the decision of the Board at the request of a natural or legal person which had the opportunity to bring an action for annulment of that decision, in particular if it was directly and individually concerned by that decision, but had not done so within the period laid down in Article 263 TFEU.

(144) Where a court seized of proceedings against a decision by a supervisory authority has reason to believe that proceedings concerning the same processing, such as the same subject matter as regards processing by the same controller or processor, or the same cause of action, are brought before a competent court in another Member State, it should contact that court in order to confirm the existence of such related proceedings. If related proceedings are pending before a court in another Member State, any court other than the court first

如果数据主体认为其在本条例下的权利受到侵害，或监管机构未对投诉采取行动、部分或全部驳回或拒绝投诉，或在为保护数据主体权利有必要采取行动时未采取行动，则数据主体有权依据《宪章》第47条获得有效司法救济。对投诉后的调查应在特定案件适当的范围内进行，并接受司法审查。监管机构应在合理期限内将投诉的进展和结果告知数据主体。如果案件需要进一步调查或与其他监管机构协调，应向数据主体提供中间信息。为便于提交投诉，各监管机构应采取措施，例如提供也可电子填写的投诉提交表格，但不排除其他通信方式。

(142) 数据主体认为其在本条例下的权利受到侵害时，有权委托依照成员国法律设立、具有符合公共利益的法定目标且活跃于个人数据保护领域的非营利机构、组织或协会，代表其向监管机构提出投诉，代表数据主体行使司法救济权，或在成员国法律有规定时，代表数据主体行使获得赔偿的权利。成员国可规定此类机构、组织或协会在该成员国有权独立于数据主体的委托提出投诉，并有权在其有理由认为因违反本条例的个人数据处理导致数据主体权利受到侵害时获得有效司法救济。不得允许该机构、组织或协会独立于数据主体的委托代表数据主体主张赔偿。

(143) 任何自然人或法人有权依照TFEU第263条规定的条件，向法院提起撤销委员会决定的诉讼。作为此类决定的对象，希望对其提出异议的相关监管机构必须依照TFEU第263条，在收到通知后两个月内提起诉讼。如果委员会的决定直接且个别地涉及控制者、处理者或投诉人，后者可依照TFEU第263条，在决定于委员会网站公布后两个月内对这些决定提起撤销诉讼。在不影响TFEU第263条项下此项权利的情况下，每个自然人或法人应有权就监管机构对其产生法律效力的决定，向有管辖权的国内法院寻求有效司法救济。此类决定尤其涉及监管机构行使调查、纠正和授权权力，或驳回或拒绝投诉。然而，有效司法救济权不包括监管机构采取的不具有法律约束力的措施，例如监管机构发布的意见或提供的建议。针对监管机构的诉讼应向该监管机构所在成员国的法院提起，并应依照该成员国的程序法进行。这些法院应行使完整管辖权，其中包括审查与提交其审理的争议相关的所有事实和法律问题的管辖权。

投诉被监管机构驳回或拒绝的，投诉人可在同一成员国向法院提起诉讼。在与本条例适用有关的司法救济中，认为有必要对相关问题作出裁判才能作出判决的国内法院，可以，或在TFEU第267条规定的情形下，必须请求法院就欧盟法(包括本条例)的解释作出初步裁定。此外，当监管机构执行委员会决定的决定在国内法院受到质疑且委员会决定的有效性存在争议时，该国内法院无权宣布委员会决定无效，但在其认为该决定无效时，必须依照法院所解释的TFEU第267条，将有效性问题提交法院。然而，国内法院不得应自然人或法人的请求就委员会决定的有效性提交问题，如果该自然人或法人有机会对该决定提起撤销诉讼，尤其是如果该决定直接且个别地涉及其，但其未在TFEU第263条规定的期限内提起诉讼。

(144) 受理针对监管机构决定诉讼的法院如果有理由相信，涉及同一处理(例如涉及同一控制者或处理者的同一处理标的，或同一诉讼原因)的诉讼已提交另一成员国有管辖权的法院，应联系该法院以确认是否存在此类相关诉讼。如果相关诉讼正在另一成员国法院待决，则除最先受理的法院以外的任何法院

seized may stay its proceedings or may, on request of one of the parties, decline jurisdiction in favour of the court first seized if that court has jurisdiction over the proceedings in question and its law permits the consolidation of such related proceedings. Proceedings are deemed to be related where they are so closely connected that it is expedient to hear and determine them together in order to avoid the risk of irreconcilable judgments resulting from separate proceedings.

(145) For proceedings against a controller or processor, the plaintiff should have the choice to bring the action before the courts of the Member States where the controller or processor has an establishment or where the data subject resides, unless the controller is a public authority of a Member State acting in the exercise of its public powers.

(146) The controller or processor should compensate any damage which a person may suffer as a result of processing that infringes this Regulation. The controller or processor should be exempt from liability if it proves that it is not in any way responsible for the damage. The concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation. This is without prejudice to any claims for damage deriving from the violation of other rules in Union or Member State law. Processing that infringes this Regulation also includes processing that infringes delegated and implementing acts adopted in accordance with this Regulation and Member State law specifying rules of this Regulation. Data subjects should receive full and effective compensation for the damage they have suffered. Where controllers or processors are involved in the same processing, each controller or processor should be held liable for the entire damage. However, where they are joined to the same judicial proceedings, in accordance with Member State law, compensation may be apportioned according to the responsibility of each controller or processor for the damage caused by the processing, provided that full and effective compensation of the data subject who suffered the damage is ensured. Any controller or processor which has paid full compensation may subsequently institute recourse proceedings against other controllers or processors involved in the same processing.

(147) Where specific rules on jurisdiction are contained in this Regulation, in particular as regards proceedings seeking a judicial remedy including compensation, against a controller or processor, general jurisdiction rules such as those of Regulation (EU) No 1215/2012 of the European Parliament and of the Council ([1]) should not prejudice the application of such specific rules.

(148) In order to strengthen the enforcement of the rules of this Regulation, penalties including administrative fines should be imposed for any infringement of this Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation. In a case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine. Due regard should however be given to the nature, gravity and duration of the infringement, the intentional character of the infringement, actions taken to mitigate the damage suffered, degree of responsibility or any relevant previous infringements, the manner in which the infringement became known to the supervisory authority, compliance with measures ordered against the controller or processor, adherence to a code of conduct and any other aggravating or mitigating factor. The imposition of penalties including administrative fines should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter, including effective judicial protection and due process.

(149) Member States should be able to lay down the rules on criminal penalties for infringements of this Regulation, including for infringements of national rules adopted pursuant to and within the limits of this Regulation. Those criminal penalties may also allow for the deprivation of the profits obtained through infringements of this Regulation. However, the imposition of criminal penalties for infringements of such national rules and of administrative penalties should not lead to a breach of the principle of *ne bis in idem*, as interpreted by the Court of Justice.

(150) In order to strengthen and harmonise administrative penalties for infringements of this Regulation, each supervisory authority should have the power to impose administrative fines. This Regulation should indicate

([1]) Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (OJ L 351, 20.12.2012, p. 1).

受理法院可中止其诉讼程序，或应一方当事人请求，如果首先受理的法院对相关诉讼具有管辖权且其法律允许合并此类相关诉讼，则可拒绝行使管辖权而由首先受理的法院审理。如果诉讼联系如此密切，以至于为避免因分别诉讼而产生不可调和判决的风险而宜一并审理和裁定，则诉讼被视为相关。

(145) 对于针对控制者或处理者的诉讼，原告应可选择向控制者或处理者设有机构的成员国法院或数据主体居住地法院提起诉讼，除非控制者是行使公共权力的成员国公共当局。

(146) 控制者或处理者应当赔偿任何人因处理行为违反本条例而可能遭受的任何损害。如果控制者或处理者证明其对损害不以任何方式负有责任，则应当免除责任。损害的概念应当根据法院的判例法进行广义解释，以充分反映本条例的目标。这不影响因违反欧盟法或成员国法律的其他规则而产生的任何损害赔偿请求。违反本条例的处理行为也包括违反根据本条例通过的授权法案和实施法案以及成员国法律规定本条例规则的处理行为。数据主体应当就其遭受的损害获得充分和有效的赔偿。如果控制者或处理者参与同一处理，每个控制者或处理者应当对整个损害承担责任。但是，如果根据成员国法律，他们在同一司法程序中被合并审理，则可以根据每个控制者或处理者对处理所造成的损害的责任来分摊赔偿，前提是确保遭受损害的数据主体获得充分和有效的赔偿。任何已支付全额赔偿的控制者或处理者随后可以对参与同一处理的其他控制者或处理者提起追偿程序。

(147) 如果本条例包含关于管辖权的特定规则，特别是关于针对控制者或处理者寻求包括赔偿在内的司法救济的诉讼，则一般管辖权规则，例如欧洲议会和理事会第(EU) No 1215/2012号条例(1)中的规则，不应妨碍此类特定规则的适用。

(148) 为了加强本条例规则的执行，对于任何违反本条例的行为，除监管机构根据本条例采取的适当措施之外或代替该等措施，应当处以包括行政罚款在内的处罚。在轻微违规的情况下，或者如果可能处以的罚款将对自然人构成不成比例的负担，可以发出训诫代替罚款。但是，应当适当考虑违规行为的性质、严重程度和持续时间、违规行为的故意性质、为减轻所遭受损害而采取的行动、责任程度或任何相关的先前违规行为、监管机构获悉违规行为的方式、对针对控制者或处理者所命令措施的遵守情况、对行为准则的遵守情况以及任何其他加重或减轻因素。处以包括行政罚款在内的处罚应当遵守符合欧盟法一般原则和《宪章》的适当程序保障，包括有效的司法保护和正当程序。

(149) 成员国应能够就违反本条例的行为，包括违反依据本条例并在其限制范围内通过的国家规则的行为，制定刑事处罚规则。这些刑事处罚还可以允许剥夺通过违反本条例所获得的利润。然而，对此类国家规则的违反行为施加刑事处罚和行政处罚，不应导致违反欧盟法院所解释的一事不再理原则。

(150) 为了加强和统一对本条例侵权行为的行政处罚，各监管机构应当有权处以行政罚款。本条例应当指明

(1) 欧洲议会和理事会2012年12月12日关于民商事案件管辖权和判决承认与执行的第(EU) No 1215/2012号条例(OJ L 351, 20.12.2012, p.1)。

infringements and the upper limit and criteria for setting the related administrative fines, which should be determined by the competent supervisory authority in each individual case, taking into account all relevant circumstances of the specific situation, with due regard in particular to the nature, gravity and duration of the infringement and of its consequences and the measures taken to ensure compliance with the obligations under this Regulation and to prevent or mitigate the consequences of the infringement. Where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes. Where administrative fines are imposed on persons that are not an undertaking, the supervisory authority should take account of the general level of income in the Member State as well as the economic situation of the person in considering the appropriate amount of the fine. The consistency mechanism may also be used to promote a consistent application of administrative fines. It should be for the Member States to determine whether and to which extent public authorities should be subject to administrative fines. Imposing an administrative fine or giving a warning does not affect the application of other powers of the supervisory authorities or of other penalties under this Regulation.

违规行为以及相关行政罚款的上限和设定标准，应当由主管监管机构在个别案件中考虑具体情况的所有相关情形后确定，特别应当适当考虑违规行为及其后果的性质、严重程度和持续时间，以及为确保遵守本条例规定的义务和防止或减轻违规行为后果而采取的措施。在对企业处以行政罚款时，为此目的，企业应当被理解为符合TFEU第101条和第102条的企业。在对非企业人员处以行政罚款时，监管机构在考虑适当罚款金额时应当考虑成员国的总体收入水平以及该人员的经济状况。一致性机制也可以用于促进行政罚款的一致适用。成员国应当决定公共机构是否以及在何种程度上应当受到行政罚款。处以行政罚款或发出警告不影响监管机构其他权力的行使或本条例规定的其他处罚的适用。

(151) The legal systems of Denmark and Estonia do not allow for administrative fines as set out in this Regulation. The rules on administrative fines may be applied in such a manner that in Denmark the fine is imposed by competent national courts as a criminal penalty and in Estonia the fine is imposed by the supervisory authority in the framework of a misdemeanour procedure, provided that such an application of the rules in those Member States has an equivalent effect to administrative fines imposed by supervisory authorities. Therefore the competent national courts should take into account the recommendation by the supervisory authority initiating the fine. In any event, the fines imposed should be effective, proportionate and dissuasive.

(151) 丹麦和爱沙尼亚的法律制度不允许本条例规定的行政罚款。关于行政罚款的规则可以以这样的方式适用：在丹麦，罚款由主管国家法院作为刑事处罚处以；在爱沙尼亚，罚款由监管机构在轻罪程序框架内处以，前提是这些成员国对规则的此种适用与监管机构处以的行政罚款具有同等效果。因此，主管国家法院应当考虑发起罚款的监管机构的建议。在任何情况下，所处以的罚款应当有效、相称且具有劝诫性。

(152) Where this Regulation does not harmonise administrative penalties or where necessary in other cases, for example in cases of serious infringements of this Regulation, Member States should implement a system which provides for effective, proportionate and dissuasive penalties. The nature of such penalties, criminal or administrative, should be determined by Member State law.

(152) 如果本条例未统一行政罚款，或在其他情况下有必要，例如在本条例严重侵权的情况下，成员国应实施一个规定有效、相称和具有威慑力的处罚制度。此类处罚的性质，无论是刑事还是行政，应由成员国法律确定。

(153) Member States law should reconcile the rules governing freedom of expression and information, including journalistic, academic, artistic and or literary expression with the right to the protection of personal data pursuant to this Regulation. The processing of personal data solely for journalistic purposes, or for the purposes of academic, artistic or literary expression should be subject to derogations or exemptions from certain provisions of this Regulation if necessary to reconcile the right to the protection of personal data with the right to freedom of expression and information, as enshrined in Article 11 of the Charter. This should apply in particular to the processing of personal data in the audiovisual field and in news archives and press libraries. Therefore, Member States should adopt legislative measures which lay down the exemptions and derogations necessary for the purpose of balancing those fundamental rights. Member States should adopt such exemptions and derogations on general principles, the rights of the data subject, the controller and the processor, the transfer of personal data to third countries or international organisations, the independent supervisory authorities, cooperation and consistency, and specific data-processing situations. Where such exemptions or derogations differ from one Member State to another, the law of the Member State to which the controller is subject should apply. In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly.

(153) 成员国法律应当协调关于表达和信息自由(包括新闻、学术、艺术和或文学表达)的规则与本条例规定的个人数据保护权。仅出于新闻目的或学术、艺术或文学表达目的处理个人数据，在必要时应适用本条例某些条款的减损或豁免，以协调个人数据保护权与《宪章》第11条所规定的表达和信息自由权。这尤其应适用于视听领域以及新闻档案和新闻图书馆中的个人数据处理。因此，成员国应当采取立法措施，规定平衡这些基本权利所必需的豁免和减损。成员国应当就一般原则、数据主体的权利、控制者和处理者、向第三国或国际组织传输个人数据、独立监管机构、合作与一致性以及特定数据处理情形规定此类豁免和减损。在此类豁免或减损因成员国而异的情况下，应当适用控制者所受管辖的成员国法律。为了顾及表达自由权在每个民主社会中的重要性，有必要对与该自由相关的概念(如新闻)作广义解释。

(154) This Regulation allows the principle of public access to official documents to be taken into account when applying this Regulation. Public access to official documents may be considered to be in the public interest. Personal data in documents held by a public authority or a public body should be able to be publicly disclosed by that authority or body if the disclosure is provided for by Union or Member State law to which the public authority or public body is subject. Such laws should reconcile public access to official documents and the reuse of public sector information with the right to the protection of personal data and may therefore provide for the necessary reconciliation with the right to the protection of personal data pursuant to this Regulation. The reference to public authorities and bodies should in that context include all authorities or other bodies covered by Member State law on public access to documents. Directive 2003/98/EC of the European Parliament and of the Council ([1]) leaves intact and in no way affects the level of protection of natural persons with regard to the

(154) 本条例允许在适用本条例时考虑官方文件公众获取原则。官方文件的公众获取可被视为符合公共利益。公共当局或公共机构所持有文件中的个人数据，如果公共当局或公共机构所受管辖的Union或成员国法律规定了披露，则该当局或机构应当能够公开披露该数据。此类法律应当协调官方文件的公众获取和公共部门信息的再利用与个人数据保护权，因此可以规定根据本条例与个人数据保护权进行必要的协调。在此背景下，对公共当局和机构的提及应当包括成员国关于文件公众获取的法律所涵盖的所有当局或其他机构。欧洲议会和理事会Directive 2003/98/EC(1)保持不变，且绝不影响自然人在以下方面获得的保护水平：

([1]) Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information (OJ L 345, 31.12.2003, p. 90).

(1) 欧洲议会和理事会2003年11月17日关于公共部门信息再利用的第2003/98/EC号指令(OJ L 345, 31.12.2003, p.90)。

processing of personal data under the provisions of Union and Member State law, and in particular does not alter the obligations and rights set out in this Regulation. In particular, that Directive should not apply to documents to which access is excluded or restricted by virtue of the access regimes on the grounds of protection of personal data, and parts of documents accessible by virtue of those regimes which contain personal data the re-use of which has been provided for by law as being incompatible with the law concerning the protection of natural persons with regard to the processing of personal data.

(155) Member State law or collective agreements, including 'works agreements', may provide for specific rules on the processing of employees' personal data in the employment context, in particular for the conditions under which personal data in the employment context may be processed on the basis of the consent of the employee, the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

(156) The processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be subject to appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation. Those safeguards should ensure that technical and organisational measures are in place in order to ensure, in particular, the principle of data minimisation. The further processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is to be carried out when the controller has assessed the feasibility to fulfil those purposes by processing data which do not permit or no longer permit the identification of data subjects, provided that appropriate safeguards exist (such as, for instance, pseudonymisation of the data). Member States should provide for appropriate safeguards for the processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. Member States should be authorised to provide, under specific conditions and subject to appropriate safeguards for data subjects, specifications and derogations with regard to the information requirements and rights to rectification, to erasure, to be forgotten, to restriction of processing, to data portability, and to object when processing personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. The conditions and safeguards in question may entail specific procedures for data subjects to exercise those rights if this is appropriate in the light of the purposes sought by the specific processing along with technical and organisational measures aimed at minimising the processing of personal data in pursuance of the proportionality and necessity principles. The processing of personal data for scientific purposes should also comply with other relevant legislation such as on clinical trials.

(157) By coupling information from registries, researchers can obtain new knowledge of great value with regard to widespread medical conditions such as cardiovascular disease, cancer and depression. On the basis of registries, research results can be enhanced, as they draw on a larger population. Within social science, research on the basis of registries enables researchers to obtain essential knowledge about the long-term correlation of a number of social conditions such as unemployment and education with other life conditions. Research results obtained through registries provide solid, high-quality knowledge which can provide the basis for the formulation and implementation of knowledge-based policy, improve the quality of life for a number of people and improve the efficiency of social services. In order to facilitate scientific research, personal data can be processed for scientific research purposes, subject to appropriate conditions and safeguards set out in Union or Member State law.

(158) Where personal data are processed for archiving purposes, this Regulation should also apply to that processing, bearing in mind that this Regulation should not apply to deceased persons. Public authorities or public or private bodies that hold records of public interest should be services which, pursuant to Union or Member State law, have a legal obligation to acquire, preserve, appraise, arrange, describe, communicate, promote, disseminate and provide access to records of enduring value for general public interest. Member States should also be authorised to provide for the further processing of personal data for archiving purposes, for example with a view to providing specific information related to the political behaviour under former totalitarian state regimes, genocide, crimes against humanity, in particular the Holocaust, or war crimes.

根据Union和成员国法律规定对个人数据的处理，尤其不改变本条例规定的义务和权利。特别是，该Directive不应当适用于因保护个人数据而根据获取制度被排除或限制获取的文件，以及根据这些制度可获取的文件中部分包含个人数据且法律已规定其再利用与关于在处理个人数据方面保护自然人的法律不相容的情形。

(155) 成员国法律或集体协议(包括"工作协议")可以规定就业背景下处理雇员个人数据的具体规则，特别是规定在就业背景下基于雇员同意处理个人数据的条件、招聘目的、履行雇佣合同(包括履行法律或集体协议规定的义务)、工作的管理、规划和组织、工作场所的平等与多样性、工作中的健康与安全，以及为个人或集体行使和享有与就业相关的权利和福利的目的，以及为终止雇佣关系的目的。

(156) 为符合公共利益的存档目的、科学或历史研究目的或统计目的处理个人数据，应当根据本条例对数据主体的权利和自由采取适当保障措施。这些保障措施应当确保技术性和组织性措施到位，以便尤其确保数据最小化原则。当控制者已评估通过处理不允许或不再允许识别数据主体的数据来实现这些目的的可行性，且存在适当保障措施(例如数据的假名化)时，应当为符合公共利益的存档目的、科学或历史研究目的或统计目的进一步处理个人数据。成员国应当为符合公共利益的存档目的、科学或历史研究目的或统计目的处理个人数据规定适当保障措施。应当授权成员国在特定条件下并在对数据主体采取适当保障措施的前提下，就信息要求以及更正、擦除、被遗忘、限制处理、数据可携性和反对的权利，在为符合公共利益的存档目的、科学或历史研究目的或统计目的处理个人数据时规定具体要求和减损。所涉条件和保障措施可包含数据主体行使这些权利的特定程序，如果根据特定处理所追求的目的以及旨在依照相称性和必要性原则最小化个人数据处理的技术性和组织性措施，这样做是适当的。为科学目的处理个人数据还应当遵守其他相关立法，例如关于临床试验的立法。

(157) 通过将登记册中的信息加以关联，研究人员能够就心血管疾病、癌症和抑郁症等广泛存在的医疗状况获得具有重大价值的新知识。在登记册的基础上，研究成果可以得到增强，因为它们依托于更大的人群。在社会科学领域，基于登记册的研究使研究人员能够获得关于失业和教育等若干社会状况与其他生活状况之间长期关联的重要知识。通过登记册获得的研究成果提供了可靠、高质量的知识，可为制定和实施基于知识的政策提供依据，改善许多人的生活质量，并提高社会服务的效率。为促进科学研究，可在遵守Union或成员国法律规定的适当条件和保障措施的前提下，为科学研究目的处理个人数据。

(158) 在为存档目的处理个人数据的情形下，本条例也应适用于该处理，同时应铭记本条例不应适用于已故人员。持有公共利益记录的公共当局或公共或私人机构，应是根据Union或成员国法律负有法律义务，为普遍公共利益获取、保存、评估、整理、描述、传达、推广、传播并提供对具有持久价值记录的访问服务的机构。成员国还应被授权规定为存档目的进一步处理个人数据，例如旨在提供与前极权国家政权下的政治行为、种族灭绝、危害人类罪(特别是大屠杀)或战争罪有关的特定信息。

(159) Where personal data are processed for scientific research purposes, this Regulation should also apply to that processing. For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research. In addition, it should take into account the Union's objective under Article 179(1) TFEU of achieving a European Research Area. Scientific research purposes should also include studies conducted in the public interest in the area of public health. To meet the specificities of processing personal data for scientific research purposes, specific conditions should apply in particular as regards the publication or otherwise disclosure of personal data in the context of scientific research purposes. If the result of scientific research in particular in the health context gives reason for further measures in the interest of the data subject, the general rules of this Regulation should apply in view of those measures.

(160) Where personal data are processed for historical research purposes, this Regulation should also apply to that processing. This should also include historical research and research for genealogical purposes, bearing in mind that this Regulation should not apply to deceased persons.

(161) For the purpose of consenting to the participation in scientific research activities in clinical trials, the relevant provisions of Regulation (EU) No 536/2014 of the European Parliament and of the Council ([1]) should apply.

(162) Where personal data are processed for statistical purposes, this Regulation should apply to that processing. Union or Member State law should, within the limits of this Regulation, determine statistical content, control of access, specifications for the processing of personal data for statistical purposes and appropriate measures to safeguard the rights and freedoms of the data subject and for ensuring statistical confidentiality. Statistical purposes mean any operation of collection and the processing of personal data necessary for statistical surveys or for the production of statistical results. Those statistical results may further be used for different purposes, including a scientific research purpose. The statistical purpose implies that the result of processing for statistical purposes is not personal data, but aggregate data, and that this result or the personal data are not used in support of measures or decisions regarding any particular natural person.

(163) The confidential information which the Union and national statistical authorities collect for the production of official European and official national statistics should be protected. European statistics should be developed, produced and disseminated in accordance with the statistical principles as set out in Article 338(2) TFEU, while national statistics should also comply with Member State law. Regulation (EC) No 223/2009 of the European Parliament and of the Council ([2]) provides further specifications on statistical confidentiality for European statistics.

(164) As regards the powers of the supervisory authorities to obtain from the controller or processor access to personal data and access to their premises, Member States may adopt by law, within the limits of this Regulation, specific rules in order to safeguard the professional or other equivalent secrecy obligations, in so far as necessary to reconcile the right to the protection of personal data with an obligation of professional secrecy. This is without prejudice to existing Member State obligations to adopt rules on professional secrecy where required by Union law.

(165) This Regulation respects and does not prejudice the status under existing constitutional law of churches and religious associations or communities in the Member States, as recognised in Article 17 TFEU.

(166) In order to fulfil the objectives of this Regulation, namely to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and to ensure the free movement

([1]) Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC (OJ L 158, 27.5.2014, p. 1).

([2]) Regulation (EC) No 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No 1101/2008 of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) No 322/97 on Community Statistics, and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities (OJ L 87, 31.3.2009, p. 164).

(159) 在为科学研究目的处理个人数据的情形下，本条例也应适用于该处理。为本条例之目的，为科学研究目的处理个人数据应作广义解释，包括例如技术开发和示范、基础研究、应用研究和私人资助的研究。此外，还应考虑Union在TFEU第179(1)条下实现欧洲研究区的目标。科学研究目的还应包括在公共卫生领域为公共利益开展的研究。为满足为科学研究目的处理个人数据的特殊性，应适用特定条件，特别是在科学研究目的背景下发表或以其他方式披露个人数据方面。如果科学研究的结果，特别是在健康领域，为数据主体的利益而有理由采取进一步措施，则应针对这些措施适用本条例的一般规则。

(160) 为历史研究目的处理个人数据的，本条例也应适用于该处理。这还应包括历史研究和为家谱目的的研究，同时考虑到本条例不应适用于已故人员。

(161) 为同意参加临床试验中的科学研究活动之目的，应适用欧洲议会和理事会(EU) No 536/2014号条例(1)的相关规定。

(162) 在为统计目的处理个人数据的情形下，本条例应适用于该处理。Union或成员国法律应在本条例的限度内确定统计内容、访问控制、为统计目的处理个人数据的规范，以及保障数据主体权利和自由并确保统计保密性的适当措施。统计目的指为统计调查或生成统计结果所必需的任何个人数据收集和处理操作。这些统计结果可进一步用于不同目的，包括科学研究目的。统计目的意味着为统计目的处理的结果不是个人数据，而是汇总数据，且该结果或个人数据不被用于支持针对任何特定自然人的措施或决定。

(163) Union和国家统计机构为编制官方欧洲统计数据和官方国家统计数据而收集的机密信息应受到保护。欧洲统计数据应按照TFEU第338(2)条规定的统计原则进行开发、编制和传播，而国家统计数据还应遵守成员国法律。欧洲议会和理事会第(EC) No 223/2009号条例(2)对欧洲统计数据的统计保密性作出了进一步规定。

(164) 关于监管机构从控制者或处理者处获取个人数据及进入其场所的权力，成员国可在本条例范围内通过法律制定具体规则，以保障职业保密或其他同等保密义务，且在协调个人数据保护权与职业保密义务所必需的范围内。此不影响成员国在欧盟法要求下制定职业保密规则的现有义务。

(165) 本条例尊重且不影响成员国中教会和宗教协会或团体依现有宪法法律所享有的地位，如TFEU第17条所承认的。

(166) 为履行本条例的目标，即保护自然人的基本权利和自由，特别是其个人数据受保护的权利，并确保自由流动

(1) 欧洲议会和理事会2014年4月16日关于人用药品临床试验并废止指令2001/20/EC的(EU)第536/2014号条例(OJ L 158, 27.5.2014, p.1)。

(2) 欧洲议会和理事会2009年3月11日关于欧洲统计的第223/2009号条例(EC)，废止欧洲议会和理事会关于向欧洲共同体统计局传输受统计保密约束的数据的第1101/2008号条例(EC, Euratom)、关于共同体统计的理事会第322/97号条例(EC)以及设立欧洲共同体统计方案委员会的理事会第89/382/EEC, Euratom号决定(OJ L 87, 31.3.2009, p.164)。

of personal data within the Union, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission. In particular, delegated acts should be adopted in respect of criteria and requirements for certification mechanisms, information to be presented by standardised icons and procedures for providing such icons. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level. The Commission, when preparing and drawing-up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and to the Council.

(167) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission when provided for by this Regulation. Those powers should be exercised in accordance with Regulation (EU) No 182/2011. In that context, the Commission should consider specific measures for micro, small and medium-sized enterprises.

(168) The examination procedure should be used for the adoption of implementing acts on standard contractual clauses between controllers and processors and between processors; codes of conduct; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country, a territory or a specified sector within that third country, or an international organisation; standard protection clauses; formats and procedures for the exchange of information by electronic means between controllers, processors and supervisory authorities for binding corporate rules; mutual assistance; and arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board.

(169) The Commission should adopt immediately applicable implementing acts where available evidence reveals that a third country, a territory or a specified sector within that third country, or an international organisation does not ensure an adequate level of protection, and imperative grounds of urgency so require.

(170) Since the objective of this Regulation, namely to ensure an equivalent level of protection of natural persons and the free flow of personal data throughout the Union, cannot be sufficiently achieved by the Member States and can rather, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union (TEU). In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

(171) Directive 95/46/EC should be repealed by this Regulation. Processing already under way on the date of application of this Regulation should be brought into conformity with this Regulation within the period of two years after which this Regulation enters into force. Where processing is based on consent pursuant to Directive 95/46/EC, it is not necessary for the data subject to give his or her consent again if the manner in which the consent has been given is in line with the conditions of this Regulation, so as to allow the controller to continue such processing after the date of application of this Regulation. Commission decisions adopted and authorisations by supervisory authorities based on Directive 95/46/EC remain in force until amended, replaced or repealed.

(172) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on 7 March 2012 ([1]).

(173) This Regulation should apply to all matters concerning the protection of fundamental rights and freedoms *vis-à-vis* the processing of personal data which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC of the European Parliament and of the Council ([2]), including the obligations on the controller and the rights of natural persons. In order to clarify the relationship between this Regulation and Directive 2002/58/EC, that Directive should be amended accordingly. Once this Regulation is adopted, Directive 2002/58/EC should be reviewed in particular in order to ensure consistency with this Regulation,

([1]) OJ C 192, 30.6.2012, p. 7.
([2]) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

对于欧盟内的个人数据，应授予委员会根据TFEU第290条通过法案的权力。特别是，应就认证机制的标准和要求、标准化图标所呈现的信息以及提供此类图标的程序通过授权法案。委员会在其准备工作中进行适当磋商，包括在专家层面，尤为重要。委员会在准备和起草授权法案时，应确保同时、及时和适当地向欧洲议会和理事会传输相关文件。

(167) 为确保实施本条例的统一条件，在本条例有规定时，应授予委员会实施权力。该等权力应依照(EU) No 182/2011号条例行使。在此背景下，委员会应考虑针对微型、小型和中型企业的具体措施。

(168) 实施法案的通过应采用审查程序，涉及控制者与处理者之间以及处理者之间的标准合同条款；行为准则；认证的技术标准和机制；第三国、该第三国境内的特定地区或部门或国际组织提供的适当保护水平；标准保护条款；控制者、处理者和监管机构之间为有约束力的公司规则以电子方式交换信息的格式和程序；互助；以及监管机构之间以及监管机构与委员会之间以电子方式交换信息的安排。

(169) 在现有证据表明第三国、该第三国内的特定领土或特定部门或国际组织不确保充分保护水平，且紧迫性要件有此要求时，委员会应立即通过适用的实施法案。

(170) 由于本条例的目标，即确保对自然人的同等保护水平以及个人数据在整个欧盟内的自由流动，无法由成员国充分实现，而由于行动的规模或影响，在欧盟层面能更好地实现，因此欧盟可根据《欧洲联盟条约》(TEU)第5条规定的辅助性原则采取措施。根据该条规定的比例性原则，本条例不超过实现该目标所必需的范围。

(171) 本 Regulation 应废除 Directive 95/46/EC。在本 Regulation 适用之日已经进行的处理，应当在本 Regulation 生效后的两年内使其符合本 Regulation。如果处理是依据 Directive 95/46/EC 基于同意进行的，则只要给予同意的方式符合本 Regulation 的条件，数据主体无需再次给予其同意，以便控制者在本 Regulation 适用之日后继续此类处理。委员会根据 Directive 95/46/EC 通过的决定以及监管机构作出的授权，在修订、替换或废除之前继续有效。

(172) 已根据(EC) No 45/2001条例第28(2)条咨询欧洲数据保护监督员，其于2012年3月7日发表了意见(1)。

(173) 本条例应适用于所有涉及保护基本权利和自由免受个人数据处理影响的事项，前提是这些事项不受欧洲议会和理事会指令2002/58/EC(2)中规定的具有相同目标的具体义务约束，包括控制者的义务和自然人的权利。为澄清本条例与该指令之间的关系，应对该指令作出相应修订。本条例通过后，应特别审查指令2002/58/EC，以确保与本条例保持一致，

(1) OJ C 192, 30.6.2012, p. 7。
(2) 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2002/58/EC号指令(隐私和电子通信指令)(OJ L 201, 31.7.2002, p.37)。

HAVE ADOPTED THIS REGULATION:

CHAPTER I

General provisions

Article 1

Subject-matter and objectives

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

Article 2

Material scope

1. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Regulation does not apply to the processing of personal data:

(a) in the course of an activity which falls outside the scope of Union law;

(b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;

(c) by a natural person in the course of a purely personal or household activity;

(d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

3. For the processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EC) No 45/2001 applies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data shall be adapted to the principles and rules of this Regulation in accordance with Article 98.

4. This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.

Article 3

Territorial scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

兹通过本 REGULATION:

第一章

一般规定

第1条

主题事项与目标

1. 本条例规定有关在个人数据处理方面保护自然人的规则以及有关个人数据自由流动的规则。

2. 本条例保护自然人的基本权利和自由，特别是其个人数据受保护的权利。

3. 不得以与在个人数据处理方面保护自然人有关的理由，限制或禁止个人数据在联盟内的自由流动。

第2条

物质范围

1. 本条例适用于全部或部分以自动化方式处理个人数据，以及以非自动化方式处理构成档案系统一部分或意图构成档案系统一部分的个人数据。

2. 本条例不适用于下列个人数据处理：

(a) 在属于欧盟法范围之外的活动过程中；(b) 由成员国在开展属于 TEU 第五编第 2 章范围内的活动时；(c) 由自然人在纯属个人或家庭活动的过程中；(d) 由主管机关为预防、调查、侦查或起诉刑事犯罪或执行刑事处罚之目的，包括为防范和预防对公共安全的威胁。

3. 对于联盟机构、机关、办事处和机构处理个人数据，适用(EC) No 45/2001号条例。(EC) No 45/2001号条例以及适用于该等个人数据处理的其他联盟法律行为，应依照Article 98调整以符合本条例的原则和规则。

4. 本条例不影响2000/31/EC号指令的适用，特别是该指令Articles 12至15中关于中介服务提供者责任规则的规定。

第3条

地域适用范围

1. 本条例适用于在控制者或处理者在联盟内的设立机构活动背景下处理个人数据，无论该处理是否发生在联盟内。

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

Article 4

Definitions

For the purposes of this Regulation:

(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(2) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

(3) 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;

(4) 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

(5) 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

(6) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

(7) 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

(8) 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

(9) 'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the

2. 本条例适用于未在欧盟设立的控制者或处理者对在欧盟内的数据主体的个人数据进行的处理，前提是处理活动涉及：

(a) 向欧盟内的此类数据主体提供商品或服务，无论是否要求数据主体付款；或

(b) 对其行为进行监控，只要其行为发生在欧盟境内。

3. 本条例适用于未在欧盟设立、但根据国际公法适用成员国法律的地方的控制者对个人数据的处理。

第4条

定义

就本条例而言：

(1) “个人数据”是指与已识别或可识别的自然人(“数据主体”)有关的任何信息；可识别的自然人是指可以直接或间接识别的自然人，特别是通过参照诸如姓名、身份证号码、位置数据、在线标识符等标识符，或通过参照该自然人的身体、生理、遗传、心理、经济、文化或社会身份的一个或多个特定因素而可识别的自然人；

(2) “处理”是指对个人数据或个人数据集合进行的任何操作或一系列操作，无论是否通过自动化方式进行，例如收集、记录、组织、结构化、存储、改编或更改、检索、查阅、使用、通过传输披露、传播或以其他方式提供、对齐或组合、限制、擦除或销毁；

(3) “限制处理”是指对存储的个人数据进行标记，以限制其未来的处理；

(4) “画像”是指对个人数据进行的任何形式的自动化处理，包括使用个人数据来评估与自然人有关的某些个人方面，特别是分析和预测该自然人的工作表现、经济状况、健康、个人偏好、兴趣、可靠性、行为、位置或移动等方面的内容；

(5) “假名化”是指以这样一种方式处理个人数据，即在不使用附加信息的情况下，个人数据不再能归属于特定数据主体，前提是此类附加信息被单独保存，并受到技术和组织措施的约束，以确保个人数据不被归属于已识别或可识别的自然人；

(6) “档案系统”是指任何按特定标准可访问的结构化个人数据集合，无论是集中式、分散式还是按功能或地理分散的；

(7) “控制者”是指单独或与他人共同确定个人数据处理的目的和方式的自然人、法人、公共机构、行政机关或其他团体；如果此类处理的目的和方式由欧盟或成员国法律确定，则控制者或其提名的具体标准可由欧盟或成员国法律规定；

(8) “处理者”是指代表控制者处理个人数据的自然人、法人、公共机构、行政机关或其他团体；

(9) “接收方”是指个人数据被披露给的自然人、法人、公共机构、行政机关或其他团体，无论是否为第三方。但是，在

framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

(10) 'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

(11) 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

(12) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

(13) 'genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

(14) 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

(15) 'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

(16) 'main establishment' means:

(a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;

(b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;

(17) 'representative' means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;

(18) 'enterprise' means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

(19) 'group of undertakings' means a controlling undertaking and its controlled undertakings;

(20) 'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

(21) 'supervisory authority' means an independent public authority which is established by a Member State pursuant to Article 51;

根据欧盟或成员国法律进行特定调查的框架内可能接收个人数据的公共机构不应被视为接收方；这些公共机构对这些数据的处理应符合根据处理目的适用的数据保护规则；

(10) "第三方"是指除数据主体、控制者、处理者以及在控制者或处理者的直接授权下被授权处理个人数据的人员之外的自然人、法人、公共机构、行政机关或团体；

(11) 数据主体的"同意"是指数据主体通过声明或明确的肯定行动，自由给出的、具体的、知情的和明确无误的意愿表示，表明其同意处理与其有关的个人数据；

(12) "个人数据泄露"是指导致传输、存储或以其他方式处理的个人数据被意外或非法销毁、丢失、更改、未经授权披露或访问的安全漏洞；

(13) "遗传数据"是指与自然人的遗传或获得的遗传特征有关的个人数据，这些特征提供关于该自然人生理或健康的独特信息，特别是来自对有关自然人的生物样本的分析；

(14) "生物识别数据"是指通过对自然人的身体、生理或行为特征进行特定技术处理而产生的个人数据，这些数据允许或确认对该自然人的唯一识别，例如面部图像或指纹数据；

(15) "健康相关数据"是指与自然人的身体或精神健康有关的个人数据，包括提供医疗保健服务，这些数据揭示有关其健康状况的信息；

(16) "主要营业机构"指：

(a) 对于在多个成员国设有机构的控制者，指其在欧盟内的中央管理机构所在地，除非关于个人数据处理目的和方式的决定由该控制者在欧盟内的另一机构作出，且后一机构有权实施此类决定，在此情况下，作出此类决定的机构应被视为主要机构；

(b) 对于在多个成员国设有机构的处理者，指其在欧盟内的中央管理机构所在地，或者，如果处理者在欧盟内没有中央管理机构，则指处理者在欧盟内的机构，在该机构的活动背景下主要处理活动发生地，前提是处理者受本条例下特定义务的约束；

(17) "代表"是指设在欧盟内的自然人、法人，由控制者或处理者根据Article 27以书面形式指定，代表控制者或处理者履行其在本条例下的各自义务；

(18) "企业"是指从事经济活动的自然人、法人，无论其法律形式如何，包括定期从事经济活动的合伙企业或协会；

(19) "企业集团"是指控制企业及其受控企业；

(20) "有约束力的公司规则"是指在一成员国领土内设立的控制者或处理者为在一个企业集团或从事联合经济活动的企业集团内向一个或多个第三国的控制者或处理者转移或一系列转移个人数据而遵守的个人数据保护政策；

(21) "监管机构"是指成员国根据Article 51设立的独立公共机构；

(22) 'supervisory authority concerned' means a supervisory authority which is concerned by the processing of personal data because:

(a) the controller or processor is established on the territory of the Member State of that supervisory authority;

(b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or

(c) a complaint has been lodged with that supervisory authority;

(23) 'cross-border processing' means either:

(a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or

(b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

(24) 'relevant and reasoned objection' means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;

(25) 'information society service' means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council [1];

(26) 'international organisation' means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

CHAPTER II

Principles

Article 5

Principles relating to processing of personal data

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

[1] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1).

(22) "相关监管机构"是指因以下原因与个人数据处理相关的监管机构：

(a) 控制者或处理者设在该监管机构的成员国领土内；

(b) 居住在该监管机构成员国的数据主体受到或可能受到处理的实质性影响；或

(c) 已向该监管机构提出投诉；

(23) "跨境处理"是指以下任一情形：

(a) 控制者或处理者在欧盟境内多个成员国设有机构，且个人数据处理是在该多个成员国机构的活动背景下进行的；或

(b) 个人数据的处理发生在控制者或处理者在欧盟单一机构的活动背景下，但实质性影响或可能实质性影响多个成员国的数据主体。

(24) "相关且有理由的异议"是指对关于是否存在违反本条例的行为，或对控制者或处理者拟采取的行动是否符合本条例的决定草案提出的异议，该异议清楚地表明决定草案对数据主体的基本权利和自由以及(在适用情况下)欧盟内个人数据自由流动所构成风险的重要性；

(25) "信息社会服务"是指欧洲议会和理事会Directive (EU) 2015/1535第1(1)条第(b)点所定义的服务；

(26) "国际组织"是指受国际公法管辖的组织及其下属机构，或由两个或两个以上国家之间的协议设立或基于该协议设立的任何其他机构。

第二章

原则

第5条

个人数据处理相关原则

1. 个人数据应：

(a) 以合法、公平和透明的方式对数据主体进行处理("合法性、公平性和透明")；

(b) 为特定、明确和正当的目的收集，且不以与这些目的不相容的方式进一步处理；为公共利益、科学或历史研究目的或统计目的进行存档的进一步处理，依照Article 89(1)，不应被视为与初始目的不相容("目的限制")；

(c) 充分、相关且限于处理目的所必需的范围("数据最小化")；

(d) 准确，并在必要时保持最新；必须采取一切合理步骤，确保考虑到处理目的，不准确的个人数据被及时删除或更正("准确性")；

(1) 欧洲议会和理事会2015年9月9日关于在技术法规和信息社会服务规则领域建立信息提供程序的Directive (EU) 2015/1535(OJ L 241, 17.9.2015, p.1)。

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Article 6

Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:

(a) Union law; or

(b) Member State law to which the controller is subject.

The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific

(e) 以允许识别数据主体的形式保存，保存期限不超过处理个人数据所需的目的所必需的期限；如果个人数据仅用于公共利益、科学或历史研究目的或统计目的存档，且符合Article 89(1)的规定，并实施本 Regulation 所要求的适当技术和组织措施以保障数据主体的权利和自由，则个人数据可保存更长时间("存储限制");

(f) 以确保个人数据适当安全的方式处理，包括使用适当的技术或组织措施防止未经授权或非法的处理以及防止意外丢失、销毁或损坏("完整性和保密性")。

2. 控制者应负责并能够证明遵守第1款（"问责"）。

第6条

处理的合法性

1. 处理仅在至少满足以下一项条件的情况下才是合法的：

(a) 数据主体已同意为其一项或多项特定目的处理其个人数据；(b) 处理对于履行数据主体作为一方的合同是必要的，或为了在订立合同前应数据主体请求采取措施是必要的；

(c) 处理对于遵守控制者所承担的法律义务是必要的；

(d) 处理对于保护数据主体或另一自然人的重大利益是必要的；(e) 处理对于执行公共利益任务或行使赋予控制者的官方权力是必要的；

(f) 处理对于控制者或第三方追求的正当利益目的是必要的，除非这些利益被数据主体的利益或基本权利和自由所压倒，且后者要求保护个人数据，特别是在数据主体是儿童的情况下。

第一项第(f)点不适用于公共机构在执行其任务时进行的处理。

2.成员国可以维持或引入更具体的规定，以调整本条例规则对第1款第(c)点和第(e)点合规处理的适用，通过更精确地确定处理的具体要求和其他措施以确保合法和公平的处理，包括Chapter IX规定的其他特定处理情形。

3. 第1款第(c)点和第(e)点所述的处理依据应由以下规定：

(a) 联盟法；或

(b) 控制者所受约束的成员国法律。

处理目的应由该法律依据确定，或者，对于paragraph 1中point (e)所述的处理，应为执行公共利益任务或行使控制者所赋予的官方权力所必需。该法律依据可包含具体规定以调整本 Regulation 规则的适用，尤其是：控制者处理合法性的一般条件；受处理的数据类型；相关数据主体；个人数据可向其披露的实体及披露目的；目的限制；存储期限；以及处理操作和处理程序，包括确保合法和公平处理的措施，例如针对其他特定

processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;

(d) the possible consequences of the intended further processing for data subjects;

(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Article 7

Conditions for consent

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

4. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Article 8

Conditions applicable to child's consent in relation to information society services

1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.

Chapter IX规定的处理情形。欧盟或成员国法律应满足公共利益目标，并与所追求的正当目的相称。

4. 如果为个人数据收集目的之外的其他目的进行的处理并非基于数据主体的同意，也非基于构成民主社会中为保障Article 23(1)所述目标所必需且相称措施的 Union 或成员国法律，则控制者为确定另一目的的处理是否与最初收集个人数据的目的相容，应尤其考虑：

(a) 收集个人数据的目的与预期进一步处理的目的之间的任何联系；

(b) 收集个人数据的情境，特别是关于数据主体与控制者之间的关系；

(c) 个人数据的性质，特别是是否依照Article 9处理特殊类别的个人数据，或是否依照Article 10处理与刑事定罪和犯罪有关的个人数据；

(d) 预期进一步处理对数据主体可能造成的后果；

(e) 是否存在适当的保障措施，其中可能包括加密或假名化。

第7条

同意的条件

1.在处理基于同意的情况下，控制者应能够证明数据主体已同意处理其个人数据。

2.如果数据主体的同意是在还涉及其他事项的书面声明的情境中给出的，同意请求应以与其他事项明显区分的方式呈现，以可理解和易于获取的形式，使用清晰和简明的语言。该声明中构成违反本条例的任何部分不具有约束力。

3.数据主体有权随时撤回其同意。撤回同意不影响在撤回前基于同意的处理的合法性。在给予同意之前，数据主体应被告知此事。撤回同意应如同给予同意一样容易。

4. 在评估同意是否自由作出时，应特别考虑，除其他外，合同的履行(包括服务的提供)是否以同意处理对该合同履行并非必要的个人数据为条件。

第8条

与信息社会服务相关的儿童同意的适用条件

1. 当Article 6(1) point (a)适用时，就向儿童直接提供信息社会服务而言，儿童至少年满16岁时，处理该儿童的个人数据应为合法。儿童未满16岁的，仅在对该儿童享有父母责任的持有人同意或授权的情况下，且在该同意或授权的范围内，该处理方为合法。

成员国可为此类目的通过法律规定的更低的年龄，但该更低的年龄不得低于13岁。

2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.

Article 9

Processing of special categories of personal data

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

2. 在此类情况下，控制者应考虑现有技术，作出合理努力以核实同意是否由对该儿童享有父母责任的持有人作出或授权。

3. 第1款不影响成员国的一般合同法，例如关于与儿童有关的合同的有效性、订立或效力的规则。

第9条

特殊类别个人数据的处理

1. 禁止处理揭示种族或民族出身、政治观点、宗教或哲学信仰或工会成员身份的个人数据，以及为唯一识别自然人之目的处理遗传数据、生物识别数据、有关健康的数据或有关自然人性生活或性取向的数据。

2. 如果下列情形之一适用，则第1款不适用：

(a) 数据主体已为一个或多个特定目的明确同意处理该等个人数据，但Union或Member State法律禁止数据主体解除第1款所述禁止的除外；

(b) 处理对于控制者或数据主体在就业、社会保障和社会保护法领域履行义务和行使特定权利是必要的，且该处理经Union或Member State法律授权，或依据Member State法律作出的、规定对数据主体的基本权利和利益提供适当保障的集体协议授权；

(c) 处理对于保护数据主体或另一自然人的重大利益是必要的，且数据主体在身体上或法律上无法作出同意；

(d) 处理是由具有政治、哲学、宗教或工会目标的基金会、协会或任何其他非营利机构在其合法活动过程中以适当保障措施进行的，条件是处理仅涉及该机构的成员或前成员，或与该机构因其目的而有定期联系的人员，并且个人数据未经数据主体同意不得在该机构之外披露；

(e) 处理涉及数据主体明显已公开的个人数据；

(f) 处理对于确立、行使或抗辩法律主张是必要的，或法院在行使其司法职能时有必要；

(g) 处理基于Union或Member State法律，为重大公共利益的原因是必要的，该法律应与所追求的目标相称、尊重数据保护权的本质，并规定适当且具体的措施以保障数据主体的基本权利和利益；

(h) 处理基于Union或Member State法律或依据与卫生专业人员的合同，为预防或职业医学、评估雇员的工作能力、医学诊断、提供卫生或社会照护或治疗或管理卫生或社会照护系统和服务的目的是必要的，并受第3款所述条件和保障的约束；

(i) 处理基于Union或Member State法律，为公共卫生领域的公共利益原因是必要的，例如防止严重的跨境健康威胁或确保卫生保健以及药品或医疗器械的高质量和安全标准，该法律应规定适当且具体的措施以保障数据主体的权利和自由，特别是职业保密；

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

Article 10

Processing of personal data relating to criminal convictions and offences

Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

Article 11

Processing which does not require identification

1. If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.

2. Where, in cases referred to in paragraph 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 15 to 20 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.

CHAPTER III

Rights of the data subject

Section 1

Transparency and modalities

Article 12

Transparent information, communication and modalities for the exercise of the rights of the data subject

1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

(j) 处理为公共利益存档目的、科学或历史研究目的或统计目的，依照Article 89(1)是必要的，且基于Union或Member State法律，该法律应与所追求的目标相称、尊重数据保护权的本质，并规定适当且具体的措施以保障数据主体的基本权利和利益。

3. 第1款所述个人数据可为第2款point (h)所述目的而处理，当该等数据由受Union或Member State法律或国家主管机构制定的规则下职业保密义务约束的专业人员处理或在其责任下处理，或由同样受Union或Member State法律或国家主管机构制定的规则下保密义务约束的另一人处理或在其责任下处理。

4. 成员国可维持或引入关于处理遗传数据、生物识别数据或有关健康的数据的进一步条件，包括限制。

第10条

处理与刑事定罪和犯罪有关的个人数据

基于Article 6(1)处理与刑事定罪和犯罪或相关安全措施有关的个人数据，仅应在官方机构的控制下进行，或在该处理经Union或Member State法律授权且该法律规定对数据主体的权利和自由提供适当保障时进行。任何刑事定罪的综合登记册应仅在官方机构的控制下保存。

第11条

无需识别身份的处理

1. 如果控制者处理个人数据的目的不要求或不再要求控制者识别数据主体，则控制者没有义务仅为遵守本条例之目的而维护、获取或处理额外信息以识别数据主体。

2. 在本条Article第1款所述情况下，如果控制者能够证明其无法识别数据主体，则控制者应在可能的情况下相应告知数据主体。在此类情况下，Articles 15 to 20不适用，除非数据主体为行使其在那些条款下的权利而提供使其能够被识别的额外信息。

第三章

数据主体的权利

第1节

透明性与方式

第12条

透明信息和通信以及数据主体行使权利的方式
主体

1. 控制者应采取适当措施，以简洁、透明、易懂和易于获取的形式，使用清晰平实的语言向数据主体提供Articles 13和14所述任何信息以及Articles 15至22和34项下与处理有关的任何通信，尤其是专门针对儿童的信息。信息应以书面形式或其他方式提供，包括在适当情况下以电子方式提供。应数据主体请求，信息可以口头提供，但须通过其他方式证明数据主体的身份。

2. The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.

3. The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

4. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

(b) refuse to act on the request.

The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

6. Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

7. The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of determining the information to be presented by the icons and the procedures for providing standardised icons.

Section 2

Information and access to personal data

Article 13

Information to be provided where personal data are collected from the data subject

1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

2. 控制者应便利数据主体行使Articles 15 to 22下的权利。在Article 11(2)所述情况下，控制者不得拒绝就数据主体为行使其在Articles 15 to 22下的权利而提出的请求采取行动，除非控制者证明其无法识别数据主体。

3. 对于数据主体依据第15条至第22条提出的请求，控制者应当毫不迟延地提供关于所采取行动的信息，且在任何情况下应在收到请求后一个月内提供。在考虑到请求的复杂性和数量的情况下，必要时该期限可再延长两个月。控制者应在收到请求后一个月内将任何此类延期通知数据主体，并说明延迟的原因。如果数据主体以电子形式提出请求，则应在可能的情况下以电子方式提供信息，除非数据主体另有要求。

4. 如果控制者未就数据主体的请求采取行动，控制者应毫不迟延地且最迟在收到请求后one month内告知数据主体未采取行动的理由以及向监管机构提出投诉和寻求司法救济的可能性。

5. 根据Articles 13 and 14提供的信息以及根据Articles 15 to 22 and 34进行的任何通信和采取的任何行动应免费提供。如果数据主体的请求明显无根据或过度，特别是因其重复性，控制者可以：

(a) 收取合理费用，同时考虑提供信息或通信或采取所请求行动的行政成本；或

(b) 拒绝按该请求行事。

控制者应承担证明请求明显无根据或过度的举证责任。

6. 在不影响Article 11的情况下，如果控制者对提出Articles 15 to 21所述请求的自然人的身份有合理怀疑，控制者可要求提供确认数据主体身份所必需的额外信息。

7. 依据第13条和第14条应向数据主体提供的信息，可以与标准化图标结合提供，以便以易于看见、易懂且清晰易读的方式，对预期处理作出有意义的概述。图标以电子方式呈现时，应具有机器可读性。

8. 为确定图标所呈现的信息以及提供标准化图标的程序，应依据第92条授权委员会通过授权法案。

第2节

信息与个人数据的访问

第13条

从数据主体处收集个人数据时应提供的信息

1. 从数据主体处收集与数据主体有关的个人数据时，控制者应在获取个人数据时向数据主体提供以下全部信息：

(a) 控制者的身份和联系方式，以及适用时控制者代表的身份和联系方式；

(b) 适用时数据保护官的联系方式；(c) 个人数据预期用于的处理目的以及处理的法律依据；

(d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

(c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(d) the right to lodge a complaint with a supervisory authority;

(e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

(f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.

Article 14

Information to be provided where personal data have not been obtained from the data subject

1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) the categories of personal data concerned;

(e) the recipients or categories of recipients of the personal data, if any;

(d) 处理基于第6(1)条(f)项时，控制者或第三方追求的正当利益；

(e) 个人数据的接收者或接收者类别(如有)；

(f) 适用时，控制者拟将个人数据转移至第三国或国际组织的事实，以及委员会充分性认定存在与否，或在第46条或第47条或第49(1)条第二款所述转移的情况下，提及适当或合适的保障措施以及获取其副本的方式或已提供这些保障措施的地点。

2. 除第1款所述信息外，控制者应在获取个人数据时向数据主体提供以下为确保公平和透明处理所必需的进一步信息：

(a) 个人数据的存储期限，或无法确定时用于确定该期限的标准；

(b) 存在向控制者请求访问与数据主体有关的个人数据以及更正或删除个人数据或限制处理的权利，或反对处理的权利，以及数据可携带权；

(c) 处理基于第6(1)条(a)项或第9(2)条(a)项时，存在随时撤回同意且不影响撤回前基于同意进行的处理合法性的权利；

(d) 向监管机构提出投诉的权利；

(e) 提供个人数据是法定义务还是合同义务，或是订立合同所必需的要求，以及数据主体是否有义务提供个人数据，以及未能提供此类数据可能产生的后果；

(f) 存在第22(1)条和(4)条所述包括画像在内的自动化决策，且至少在这些情况下，关于所涉逻辑的有意义信息，以及此类处理对数据主体的重要性和预期后果。

3. 控制者拟将个人数据进一步处理用于收集个人数据目的以外的其他目的时，控制者应在该进一步处理之前向数据主体提供关于该其他目的的信息以及第2款所述任何相关进一步信息。

4. 数据主体已经拥有该信息时，第1款、第2款和第3款不适用。

第14条

未从数据主体处获得个人数据时应提供的信息

1. 未从数据主体处获得个人数据时，控制者应向数据主体提供以下信息：

(a) 控制者的身份和联系方式，以及适用时控制者代表的身份和联系方式；

(b) 适用时数据保护官的联系方式；(c) 个人数据预期用于的处理目的以及处理的法律依据；(d) 所涉个人数据的类别；

(e) 个人数据的接收者或接收者类别(如有)；

(f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(c) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;

(d) where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(e) the right to lodge a complaint with a supervisory authority;

(f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;

(g) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. The controller shall provide the information referred to in paragraphs 1 and 2:

(a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;

(b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or

(c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

4. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

5. Paragraphs 1 to 4 shall not apply where and insofar as:

(a) the data subject already has the information;

(b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;

(c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or

(d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

(f) 适用时，控制者拟将个人数据转移至第三国或国际组织中的接收方，以及委员会充分性认定存在与否，或在第46条或第47条或第49(1)条第二款所述转移的情况下，提及适当或合适的保障措施以及获取其副本的方式或已提供这些保障措施的地点。

2. 除第1款所述信息外，控制者应向数据主体提供以下为确保对数据主体进行公平和透明处理所必需的信息：

(a) 个人数据的存储期限，或无法确定时用于确定该期限的标准；

(b) 处理基于第6(1)条(f)项时，控制者或第三方追求的正当利益；

(c) 存在向控制者请求访问与数据主体有关的个人数据以及更正或删除个人数据或限制处理的权利，以及反对处理的权利，以及数据可携带权；

(d) 处理基于第6(1)条(a)项或第9(2)条(a)项时，存在随时撤回同意且不影响撤回前基于同意进行的处理合法性的权利；

(e) 向监管机构提出投诉的权利；

(f) 个人数据来源，以及适用时是否来自公开可访问的来源；

(g) 存在第22(1)条和(4)条所述包括画像在内的自动化决策，且至少在这些情况下，关于所涉逻辑的有意义信息，以及此类处理对数据主体的重要性和预期后果。

3. 控制者应提供第1款和第2款所述的信息：

(a) 在获得个人数据后的合理期限内，但最迟在一个月内，同时考虑处理个人数据的具体情形；

(b) 个人数据将用于与数据主体通信时，最迟在该数据主体首次通信时；或

(c) 拟向另一接收方披露时，最迟在个人数据首次披露时。

4. 控制者拟将个人数据进一步处理用于获得个人数据目的以外的其他目的时，控制者应在该进一步处理之前向数据主体提供关于该其他目的的信息以及第2款所述任何相关进一步信息。

5. 第1至第4款在下列情形下且在此范围内不适用：

(a) 数据主体已拥有该信息；

(b) 提供此类信息被证明不可能或会涉及不成比例的努力，特别是为了公共利益、科学或历史研究目的或统计目的而进行的处理，但须符合第89(1)条所述的条件和保障措施，或者只要本条第一款所述的义务可能使该处理的目标无法实现或受到严重损害。在此类情况下，控制者应采取适当措施保护数据主体的权利和自由及正当利益，包括使信息可公开获取；

(c) 控制者所受的Union或成员国法律明确规定获取或披露，且该法律规定了保护数据主体正当利益的适当措施；或

(d) 个人数据必须根据Union或成员国法律规定的职业保密义务保密，包括法定保密义务。

Article 15

Right of access by the data subject

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(f) the right to lodge a complaint with a supervisory authority;

(g) where the personal data are not collected from the data subject, any available information as to their source;

(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

Section 3

Rectification and erasure

Article 16

Right to rectification

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Article 17

Right to erasure (‘right to be forgotten’)

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

第15条

数据主体的访问权

1. 数据主体有权从控制者处获得关于其个人数据是否正在被处理的确认，并在该等情形下，获取该个人数据以及以下信息：

(a) 处理目的；

(b) 所涉及的个人数据类别；

(c) 个人数据已经或将要披露给的接收方或接收方类别，特别是第三国或国际组织中的接收方；

(d) 在可能的情况下，个人数据将被存储的预期期限，或者，如果不可能，用于确定该期限的标准；

(e) 存在向控制者请求更正或删除个人数据或限制处理与数据主体有关的个人数据或反对该等处理的权利；

(f) 向监管机构提出投诉的权利；

(g) 在个人数据并非从数据主体处收集的情况下，关于其来源的任何可获得的信息；(h) 存在第22(1)条和第(4)条所述的自动化决策，包括画像，以及至少在该等情形下，关于所涉逻辑的有意义信息，以及该等处理对数据主体的重要性和预期后果。

2. 在个人数据被传输至第三国或国际组织的情况下，数据主体有权获知依据第46条与该传输有关的适当保障措施。

3. 控制者应提供正在处理的个人数据的副本。对于数据主体请求的任何进一步副本，控制者可基于行政成本收取合理费用。在数据主体通过电子方式提出请求的情况下，除非数据主体另有请求，信息应以常用的电子形式提供。

4. 第3款所述的获取副本的权利不得对他人的权利和自由产生不利影响。

第3节

更正与删除

第16条

更正权

数据主体有权从控制者处不受不当延迟地获得对其不准确的个人数据的更正。考虑到处理的目的，数据主体有权使不完整的个人数据完整，包括通过提供补充声明的方式。

第17条

删除权（“被遗忘权”）

1. 数据主体有权从控制者处不受不当延迟地获得对其个人数据的删除，且在以下任一理由适用时，控制者有义务不受不当延迟地删除个人数据：

(a) 个人数据对于其被收集或以其他方式处理的目的而言不再必要；

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

(a) for exercising the right of freedom of expression and information;

(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) for the establishment, exercise or defence of legal claims.

Article 18

Right to restriction of processing

1. The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

(a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

(b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

(c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

(d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

2. Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

(b) 数据主体撤回依据第6(1)条(a)点或第9(2)条(a)点作为处理依据的同意，且不存在其他处理的合法理由；

(c) 数据主体依据第21(1)条反对处理，且不存在压倒性的正当利益作为处理的依据，或者数据主体依据第21(2)条反对处理；

(d) 个人数据已被非法处理；

(e) 为遵守控制者所应遵守的Union或成员国法律中的法律义务，个人数据必须被删除；

(f) 个人数据是与第8(1)条所述的信息社会服务提供相关而收集的。

2. 在控制者已公开个人数据并有义务依据第1款删除该个人数据的情况下，控制者应考虑可用的技术和实施成本，采取合理步骤，包括技术措施，通知正在处理该个人数据的控制者数据主体已请求该等控制者删除与这些个人数据的任何链接，或副本或复制件。

3. 第1款和第2款不适用于以下情形所必需的处理：

(a) 为行使表达和信息自由的权利；(b) 为遵守要求控制者进行处理的Union或成员国法律中的法律义务，或为执行公共利益任务或行使赋予控制者的官方职权；

(c) 为公共卫生领域的公共利益原因，依据第9(2)条(h)点和(i)点以及第9(3)条；

(d) 为公共利益存档目的、科学或历史研究目的或统计目的，依据第89(1)条，只要第1款所述的权利可能使该等处理目标的实现变得不可能或受到严重损害；或

(e) 为了确立、行使或抗辩法律主张。

第18条

限制处理权

1. 在以下任一情形适用时，数据主体有权从控制者处获得对处理的限制：

(a) 个人数据的准确性由数据主体提出质疑，在此期间使控制者能够核实个人数据的准确性；

(b) 处理是非法的，且数据主体反对删除个人数据并要求限制其使用；

(c) 控制者不再需要个人数据用于处理目的，但数据主体需要这些数据用于法律主张的建立、行使或抗辩；

(d) 数据主体已依据 Article 21(1) 反对处理，等待核实控制者的正当理由是否优先于数据主体的理由。

2. 当处理已依据 paragraph 1 受到限制时，除存储外，此类个人数据仅可在数据主体同意的情况下处理，或为法律主张的建立、行使或抗辩，或为保护另一自然人或法人的权利，或为 Union 或 Member State 的重要公共利益原因而处理。

3. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

Article 19

Notification obligation regarding rectification or erasure of personal data or restriction of processing

The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

Article 20

Right to data portability

1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

(a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and

(b) the processing is carried out by automated means.

2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

Section 4

Right to object and automated individual decision-making

Article 21

Right to object

1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

3. 已依据 paragraph 1 获得处理限制的数据主体，应在处理限制解除之前由控制者告知。

第19条

关于个人数据更正或删除或限制的告知义务处理

控制者应将依据 Article 16、Article 17(1) 和 Article 18 进行的任何个人数据更正或删除或处理限制传达给个人数据已向其披露的每个接收方，除非这被证明不可能或涉及不成比例的努力。控制者应在数据主体要求时告知数据主体这些接收方。

第20条

数据可携权

1. 数据主体有权以结构化、常用和机器可读的格式接收其提供给控制者的与其相关的个人数据，并有权将这些数据传输给另一控制者，而不受个人数据已向其提供的控制者的阻碍，当：

(a) 处理基于第6(1)条(a)项或第9(2)条(a)项的同意的，或基于第6(1)条(b)项的合同的；且

(b) 处理是通过自动化方式进行的。

2. 在依据 paragraph 1 行使其数据可携带权时，数据主体有权在技术可行的情况下将个人数据从一个控制者直接传输到另一控制者。

3. 行使本 Article 的 paragraph 1 中提及的权利不应影响 Article 17。该权利不适用于为执行公共利益任务或行使赋予控制者的官方权力所必需的处理。

4. paragraph 1 中提及的权利不应对他人的权利和自由产生不利影响。

第4节

反对权和自动化个人决策

第21条

反对权

1. 数据主体有权基于与其特定情况相关的理由，随时反对依据Article 6(1)的point (e)或point (f)对其个人数据进行的处理，包括基于这些条款的画像。控制者不得再处理该个人数据，除非控制者证明存在凌驾于数据主体的利益、权利和自由之上的令人信服的正当处理理由，或为确立、行使或抗辩法律主张所必需。

2. 当个人数据为直接营销目的而处理时，数据主体有权随时反对处理与其相关的个人数据用于此类营销，包括在此类直接营销相关的范围内的画像。

3. 当数据主体反对为直接营销目的的处理时，个人数据不应再为此类目的而处理。

4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

5. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.

6. Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Article 22

Automated individual decision-making, including profiling

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

2. Paragraph 1 shall not apply if the decision:

(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

(c) is based on the data subject's explicit consent.

3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

Section 5

Restrictions

Article 23

Restrictions

1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

(a) national security;

(b) defence;

(c) public security;

4. 最迟在与数据主体首次通信时，paragraphs 1 和 2 中提及的权利应明确提请数据主体注意，并应与任何其他信息清晰分开呈现。

5. 在使用信息社会服务的背景下，尽管有 Directive 2002/58/EC，数据主体可通过使用技术规范的自动化方式行使其反对权。

6. 当个人数据依据 Article 89(1) 为科学或历史研究目的或统计目的而处理时，数据主体基于与其特定情况相关的理由，有权反对处理与其相关的个人数据，除非处理是为公共利益原因执行任务所必需的。

第22条

自动化个体决策，包括画像

1. 数据主体有权不受仅基于自动化处理(包括画像)的决定的约束，该决定对其产生法律效力或类似地显著影响其。

2. 第1款不适用于以下决定：

(a) 为数据主体与数据控制者之间订立或履行合同所必需；

(b) 由控制者所受约束的 Union 或 Member State 法律授权，且该法律还规定了适当措施以保障数据主体的权利和自由及正当利益；或

(c) 是基于数据主体的明确同意。

3. 在 paragraph 2 的 points(a) 和(c) 中提及的情况下，数据控制者应实施适当措施以保障数据主体的权利和自由及正当利益，至少包括获得控制者方面人工干预、表达其观点和质疑决定的权利。

4. paragraph 2 中提及的决定不应基于 Article 9(1) 中提及的特殊类别的个人数据，除非 point(a) 或(g) of Article 9(2) 适用且已实施适当措施以保障数据主体的权利和自由及正当利益。

第5节

限制

第23条

限制

1. 数据控制者或处理者所受约束的Union或Member State法律，可通过立法措施限制Articles 12至22和Article 34所规定的义务和权利的范围，以及Article 5中与Articles 12至22所规定的权利和义务相对应的条款，前提是此种限制尊重基本权利和自由的本质，并且是民主社会中为保障以下各项所必需且相称的措施：

(a) 国家安全；

(b) 抗辩；

(c) 公共安全；

(d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

(e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security;

(f) the protection of judicial independence and judicial proceedings;

(g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

(h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);

(i) the protection of the data subject or the rights and freedoms of others;

(j) the enforcement of civil law claims.

2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to:

(a) the purposes of the processing or categories of processing;

(b) the categories of personal data;

(c) the scope of the restrictions introduced;

(d) the safeguards to prevent abuse or unlawful access or transfer;

(e) the specification of the controller or categories of controllers;

(f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;

(g) the risks to the rights and freedoms of data subjects; and

(h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

CHAPTER IV

Controller and processor

Section 1

General obligations

Article 24

Responsibility of the controller

1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.

(d) 刑事犯罪的预防、调查、侦查或起诉或刑事处罚的执行，包括防范和预防对公共安全的威胁；

(e) Union 或 Member State 的其他重要一般公共利益目标，特别是 Union 或 Member State 的重要经济或金融利益，包括货币、预算和税收事项、公共卫生和社会保障；

(f) 保护司法独立和司法程序；

(g) 受监管职业违反道德行为的预防、调查、侦查和起诉；(h) 在 points(a) 至(e) 和(g) 中提及的情况下，与行使官方权力相关的监测、检查或监管职能，即使偶尔相关；

(i) 对数据主体的保护或他人的权利和自由；

(j) 民事法律请求的执行。

2. 特别是，paragraph 1 中提及的任何立法措施应至少包含具体规定，在相关情况下，关于：

(a) 处理目的或处理类别；

(b) 个人数据的类别；

(c) 所引入限制的范围；(d) 防止滥用或非法访问或传输的保障措施；(e) 控制者或控制者类别的指定；(f) 考虑到处理或处理类别的性质、范围和目的的存储期限和适用保障措施；

(g) 对数据主体权利和自由构成的风险；以及

(h) 数据主体有权被告知限制，除非这可能损害限制的目的。

第四章

控制者与处理者

第1节

一般义务

第24条

控制者的责任

1. 考虑到处理的性质、范围、背景和目的，以及对自然人的权利和自由造成的各种可能性和严重程度的风险，控制者应实施适当的技术和组织措施，以确保并能够证明处理是按照本条例进行的。这些措施应在必要时予以审查和更新。

2. 在与处理活动相称的情况下，第1款所述措施应包括控制者实施适当的数据保护政策。

3. 遵守第40条所述经批准的行为准则或第42条所述经批准的认证机制，可作为证明控制者遵守义务的一个要素。

Article 25

Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

Article 26

Joint controllers

1. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.

2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers *vis-à-vis* the data subjects. The essence of the arrangement shall be made available to the data subject.

3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.

Article 27

Representatives of controllers or processors not established in the Union

1. Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in the Union.

2. The obligation laid down in paragraph 1 of this Article shall not apply to:

(a) processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or

(b) a public authority or body.

第25条

默认数据保护和通过设计的数据保护

1. 考虑到现有技术水平、实施成本以及处理的性质、范围、背景和目的，以及处理对自然人的权利和自由造成的各种可能性和严重程度的风险，控制者应当在确定处理手段之时以及处理本身进行之时，实施适当的技术和组织措施，例如假名化，这些措施旨在有效落实数据保护原则(如数据最小化)，并将必要的保障措施纳入处理之中，以满足本条例的要求并保护数据主体的权利。

2. 控制者应当实施适当的技术和组织措施，以确保在默认情况下，仅处理为处理各项特定目的所必需的个人数据。该义务适用于所收集的个人数据的数量、其处理的范围、其存储的期限及其可访问性。特别是，此类措施应当确保在默认情况下，未经个人干预，个人数据不会被无限数量的自然人访问。

3. 依据第42条经批准的认证机制可作为证明符合本条第1款和第2款所规定要求的一个要素。

第26条

共同控制者

1. 当两个或两个以上的控制者共同确定处理的目的和手段时，他们应为共同控制者。他们应当以透明的方式，通过彼此之间的安排，确定各自在遵守本条例义务方面的责任，特别是关于数据主体权利的行使以及各自提供Articles 13和14所述信息的义务，除非且仅限于控制者所受约束的Union或Member State法律已确定控制者各自的责任。该安排可指定一个面向数据主体的联系点。

2. 第1款所述安排应适当反映共同控制者相对于数据主体的各自角色和关系。该安排的要点应提供给数据主体。

3. 无论第1款所述安排的条款如何，数据主体均可针对每一控制者行使本条例赋予其的权利。

第27条

未在欧盟设立的控制者或处理者的代表

1. 在适用第3(2)条的情况下，控制者或处理者应以书面形式在欧盟指定一名代表。

2. 本条第一款规定的义务不适用于：

(a) 偶尔进行、不涉及大规模处理第9(1)条所述特殊类别的数据或第10条所述与刑事定罪和犯罪有关的个人数据、且考虑到处理的性质、背景、范围和目的不太可能导致对自然人权利和自由的风险的处理；或

(b) 一个公共当局或机构。

3. The representative shall be established in one of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are.

4. The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation.

5. The designation of a representative by the controller or processor shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves.

Article 28

Processor

1. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

(a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

(b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) takes all measures required pursuant to Article 32;

(d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;

(e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

(f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;

(g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;

(h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

3. 代表应设立在以下成员国之一：其个人数据因向其提供商品或服务而被处理的数据主体，或其行为被监控的数据主体所在的成员国。

4. 控制者或处理者应授权代表，以便监管机构和数据主体就与处理相关的所有事项，在控制者或处理者之外或代替控制者或处理者向其提出，以确保对本条例的遵守。

5. 控制者或处理者指定代表不影响可对控制者或处理者本身提起的法律诉讼。

第28条

处理者

1. 当处理将代表控制者进行时，控制者应仅使用提供充分保证的处理者，以确保其以适当的技术和组织措施实施处理，使处理符合本条例的要求并确保对数据主体权利的保护。

2. 处理者不得在未经控制者事先具体或一般书面授权的情况下聘用另一处理者。在一般书面授权的情况下，处理者应将有关增加或更换其他处理者的任何预期变更通知控制者，从而使控制者有机会对此类变更提出反对。

3. 处理者进行的处理应受根据Union或成员国法律签订的合同或其他法律行为的约束，该合同或法律行为对处理者就控制者具有约束力，并规定处理的主题事项和持续时间、处理的性质和目的、个人数据的类型和数据主体的类别以及控制者的义务和权利。该合同或其他法律行为应特别规定，处理者：

(a) 仅根据控制者的书面指示处理个人数据，包括关于向第三国或国际组织传输个人数据，除非处理者所受的Union或成员国法律要求其这样做；在此种情况下，处理者应在处理前将该法律要求通知控制者，除非该法律基于公共利益的重要理由禁止此类通知；

(b) 确保获授权处理个人数据的人员已承诺保密或负有适当的法定保密义务；

(c) 采取依据 Article 32 要求的所有措施；

(d) 遵守第2款和第4款中关于聘用另一处理者的条件；

(e) 考虑到处理的性质，在可能的范围内，通过适当的技术和组织措施协助控制者履行其回应数据主体行使第三章所规定权利的请求的义务；

(f) 考虑到处理的性质和处理者可获得的信息，协助控制者确保遵守第32条至第36条规定的义务；

(g) 在与处理相关的服务提供结束后，根据控制者的选择，删除或向控制者返还所有个人数据，并删除现有副本，除非Union或成员国法律要求存储该个人数据；

(h) 向控制者提供证明遵守本条所规定义务所需的所有信息，并允许和协助控制者或控制者授权的另一审计员进行的审计，包括检查。

With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

5. Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.

6. Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 7 and 8 of this Article, including when they are part of a certification granted to the controller or processor pursuant to Articles 42 and 43.

7. The Commission may lay down standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the examination procedure referred to in Article 93(2).

8. A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the consistency mechanism referred to in Article 63.

9. The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.

10. Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

Article 29

Processing under the authority of the controller or processor

The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

Article 30

Records of processing activities

1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

(a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

(b) the purposes of the processing;

(c) a description of the categories of data subjects and of the categories of personal data;

关于第一项第(h)点，处理者如认为某项指示违反本条例或其他Union或成员国数据保护规定，应立即通知控制者。

4. 处理者代表控制者进行特定处理活动而委托另一处理者时，应通过合同或其他欧盟法或成员国法律下的法律行为，向该另一处理者施加控制者与处理者之间依据第3款在合同或其他法律行为中约定的相同数据保护义务，尤其应提供充分保证，以采取适当的技术和组织措施，使处理符合本条例的要求。该另一处理者未能履行其数据保护义务的，初始处理者仍应就该另一处理者义务的履行向控制者承担全部责任。

5. 处理者遵守第40条所指经批准的行为准则或第42条所指经批准的认证机制，可作为证明本条第1款和第4款所指充分保证的要素。

6. 在不影响控制者与处理者之间个别合同的情况下，本条第3款和第4款所指的合同或其他法律行为可全部或部分基于本条第7款和第8款所指的标准合同条款，包括当其构成根据第42条和第43条授予控制者或处理者的认证的一部分时。

7. 委员会可按照第93条第2款所指的审查程序，为本条第3款和第4款所指事项制定标准合同条款。

8. 监管机构可按照第63条所指的一致性机制，为本条第3款和第4款所指事项通过标准合同条款。

9. 第3款和第4款所指的合同或其他法律行为应采用书面形式，包括电子形式。

10. 在不影响第82条、第83条和第84条的情况下，如果处理者通过确定处理的目的和方式违反本条例，则该处理者就该处理应被视为控制者。

第29条

3.在控制者或处理者的授权下进行处理4.

处理者以及任何在控制者或处理者授权下行事且可访问个人数据的人员，除根据控制者的指示外，不得处理这些数据，除非Union或成员国法律要求其这样做。

第30条

处理活动记录

1. 每个控制者以及(如适用)控制者的代表，应保存其负责下的处理活动的记录。该记录应包含以下所有信息：

(a) 控制者以及(如适用)共同控制者、控制者的代表和数据保护官的姓名和联系方式；

(b) 处理目的；

(c) 对数据主体类别和个人数据类别的描述；

(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(f) where possible, the envisaged time limits for erasure of the different categories of data;

(g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

2. Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

(a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;

(b) the categories of processing carried out on behalf of each controller;

(c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.

4. The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.

5. The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.

Article 31

Cooperation with the supervisory authority

The controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks.

Section 2

Security of personal data

Article 32

Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;

(d) 个人数据已向其披露或将向其披露的接收方类别，包括第三国或国际组织中的接收方；

(e) 如适用，向第三国或国际组织传输个人数据的情况，包括该第三国或国际组织的标识，以及在第49条第1款第二项所指传输的情况下，适当保障措施的文档记录；

(f) 在可能的情况下，不同类别数据的预定删除时限；

(g) 在可能的情况下，对第32条第1款所指技术和组织安全措施的一般描述。

2. 每个处理者以及(如适用)处理者的代表，应保存代表控制者进行的所有处理活动类别的记录，包含：

(a) 处理者或各处理者以及处理者代表其行事的各控制者的名称和联系方式，以及在适用情况下，控制者或处理者的代表和数据保护官的名称和联系方式；

(b) 代表每个控制者进行的处理类别；

(c) 如适用，向第三国或国际组织传输个人数据的情况，包括该第三国或国际组织的标识，以及在第49条第1款第二项所指传输的情况下，适当保障措施的文档记录；

(d) 在可能的情况下，对第32条第1款所指技术和组织安全措施的一般描述。

3. 第1款和第2款所指的记录应以书面形式作出，包括电子形式。

4. 控制者或处理者，以及在适用情况下，控制者或处理者的代表，应当应要求向监管机构提供该记录。

5. 第1款和第2款所指的义务不适用于雇用少于250人的企业或组织，除非其进行的处理可能导致对数据主体的权利和自由的风险，该处理不是偶发性的，或者该处理包括第9(1)条所指的特殊类别数据或第10条所指的与刑事定罪和犯罪有关的个人数据。

第31条

与监管机构的合作

控制者和处理者，以及在适用情况下其代表，应当应要求配合监管机构履行其任务。

第2节

个人数据的安全

第32条

处理安全

1. 考虑到现有技术水平、实施成本以及处理的性质、范围、背景和目的，以及对自然人的权利和自由造成不同可能性和严重程度的风险，控制者和处理者应当实施适当的技术和组织措施，以确保与风险相适应的安全水平，其中包括在适当情况下的以下措施：

(a) 个人数据的假名化和加密；

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

Article 33

Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:

(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

(c) describe the likely consequences of the personal data breach;

(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Article 34

Communication of a personal data breach to the data subject

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

(b) 确保处理系统和服务持续保密性、完整性、可用性和韧性的能力；

(c) 在发生物理或技术事件时及时恢复个人数据可用性和访问的能力；

(d) 定期测试、评估和评价技术性和组织性措施有效性的流程，以确保处理的安全性。

2. 在评估适当的安全水平时，应特别考虑处理所带来的风险，尤其是意外或非法销毁、丢失、更改、未经授权披露或访问传输、存储或以其他方式处理的个人数据的风险。

3. 遵守第40条所指的经批准的行为准则或第42条所指的经批准的认证机制，可作为证明符合本条第1款所规定要求的要素。

4. 控制者和处理者应当采取措施，确保在控制者或处理者授权下行事的、可访问个人数据的任何自然人，除根据控制者的指示外不处理这些数据，除非Union或成员国法律要求其这样做。

第33条

向监管机构通报个人数据泄露

1. 发生个人数据泄露时，控制者应在无不合理延迟的情况下，并在可行时于知悉后不迟于72小时内，依据第55条向有管辖权的监管机构通知该个人数据泄露，除非该个人数据泄露不太可能导致自然人的权利和自由面临风险。未在72小时内向监管机构通知的，应同时说明延迟的理由。

2. 处理者在知悉个人数据泄露后，应当毫不迟延地通知控制者。

3. 第1款所述的通报至少应：

(a) 说明个人数据泄露的性质，包括在可能情况下，涉及的数据主体的类别和大致数量以及涉及的个人数据记录的类别和大致数量；

(b) 传达数据保护官或其他可获取更多信息的联系点的名称和联系方式；

(c) 描述个人数据泄露可能造成的后果；

(d) 说明控制者为应对个人数据泄露已采取或拟采取的措施，包括在适当情况下减轻其可能不利影响的措施。

4. 在无法同时提供信息的情况下，可在不造成不当进一步延迟的前提下分阶段提供信息。

5. 控制者应当记录任何个人数据泄露，包括与个人数据泄露有关的事实、其影响以及所采取的补救措施。该记录应当使监管机构能够核实对本条的遵守情况。

第34条

将个人数据泄露告知数据主体

1. 当个人数据泄露可能对自然人的权利和自由造成高风险时，控制者应当毫不迟延地将个人数据泄露告知数据主体。

2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).

3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

(a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;

(c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

Section 3

Data protection impact assessment and prior consultation

Article 35

Data protection impact assessment

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

(c) a systematic monitoring of a publicly accessible area on a large scale.

4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.

5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.

6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

2. 本条第1款所指对数据主体的告知应当以清晰平实的语言说明个人数据泄露的性质，并至少包含第33(3)条(b)、(c)和(d)项所指的信息和措施。

3. 在满足以下任一条件时，不要求进行第1款所指对数据主体的告知：

(a) 控制者已实施适当的技术和组织保护措施，且这些措施已应用于受个人数据泄露影响的个人数据，尤其是使个人数据对任何无权访问者不可理解的那些措施，例如加密；

(b) 控制者已采取后续措施，确保第1款所指对数据主体权利和自由的高风险不再可能发生；

(c) 这将涉及不成比例的努力。在此情况下，应当改为进行公开告知或类似措施，以同等有效的方式告知数据主体。

4. 如果控制者尚未将个人数据泄露告知数据主体，监管机构在考虑个人数据泄露导致高风险的可能性后，可要求其进行告知，或可决定第3款所指的任一条件已满足。

第3节

数据保护影响评估与事先咨询

第35条

数据保护影响评估

1. 当某一类型的处理，特别是使用新技术的处理，考虑到处理的性质、范围、背景和目的，可能导致对自然人的权利和自由的高风险时，控制者应当在处理前对拟进行的处理操作对个人数据保护的影响进行评估。一项评估可以涵盖一组呈现类似高风险的处理操作。

2. 控制者在进行数据保护影响评估时，应当征求数据保护官(如已指定)的意见。

3. 在以下情况下，尤其要求进行第1款所指的数据保护影响评估：

(a) 基于自动化处理(包括画像)对与自然人有关的个人方面进行系统和广泛的评估，并基于该评估作出对自然人产生法律效力或类似重大影响的决定；

(b) 大规模处理第9(1)条所指的特殊类别数据，或第10条所指的与刑事定罪和犯罪有关的个人数据；或

(c) 对可公开访问区域进行大规模系统性监控。

4. 监管机构应建立并公布一份依据第1款需要进行数据保护影响评估的处理操作类型的清单。监管机构应将这些清单通报给第68条所述委员会。

5. 监管机构还可建立并公布一份无需进行数据保护影响评估的处理操作类型的清单。监管机构应将这些清单通报给委员会。

6. 在通过第4款和第5款所述清单之前，主管监管机构应在该等清单涉及与向数据主体提供商品或服务或在多个成员国监控其行为相关的处理活动，或可能实质性影响个人数据在联盟内自由流动时，适用第63条所述一致性机制。

7. The assessment shall contain at least:

(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

8. Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.

9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

10. Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.

11. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

7. 评估应至少包含：

(a) 对拟议处理操作和处理目的的系统性描述，包括(适用时)控制者所追求的正当利益；

(b) 对处理操作相对于目的的必要性和相称性的评估；

(c) 对第1款所述数据主体权利和自由的风险的评估；以及(d) 为应对风险所设想采取的措施，包括保障措施、安全措施和确保个人数据保护并证明符合本条例的机制，同时考虑数据主体和其他相关人员的权利和正当利益。

8. 在评估相关控制者或处理者所执行处理操作的影响时，应适当考虑该等控制者或处理者遵守第40条所述经批准的行为准则的情况，特别是为数据保护影响评估之目的。

9. 在适当情况下，控制者应就拟议处理征求数据主体或其代表的意见，但不影响对商业或公共利益的保护或处理操作的安全。

10. 依据第6(1)条(c)项或(e)项进行的处理在控制者所受约束的欧盟法或成员国法律中有法律依据，该法律规范了所涉特定处理操作或一组处理操作，并且作为通过该法律依据过程中一般影响评估的一部分已经进行了数据保护影响评估的，第1款至第7款不适用，除非成员国认为有必要在处理活动之前进行此类评估。

11. 在必要时，控制者应进行审查以评估处理是否按照数据保护影响评估进行，至少在处理操作所代表的风险发生变化时。

Article 36

Prior consultation

1. The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

2. Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the supervisory authority shall, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of its powers referred to in Article 58. That period may be extended by six weeks, taking into account the complexity of the intended processing. The supervisory authority shall inform the controller and, where applicable, the processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay. Those periods may be suspended until the supervisory authority has obtained information it has requested for the purposes of the consultation.

3. When consulting the supervisory authority pursuant to paragraph 1, the controller shall provide the supervisory authority with:

(a) where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;

(b) the purposes and means of the intended processing;

(c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation;

(d) where applicable, the contact details of the data protection officer;

第36条

事先咨询

1. 当第35条下的数据保护影响评估表明，在控制者未采取措施缓解风险的情况下处理将导致高风险时，控制者应在处理前咨询监管机构。

2. 监管机构认为第1款所述预期处理将违反本条例，特别是控制者未充分识别或缓解风险的，监管机构应在收到磋商请求后最长八周的期限内，向控制者并在适用时向处理者提供书面意见，并可行使第58条所述任何权力。考虑到预期处理的复杂性，该期限可延长六周。监管机构应在收到磋商请求后一个月内，将任何此类延期连同延迟理由通知控制者并在适用时通知处理者。在监管机构获得其为磋商目的所请求的信息之前，上述期限可中止。

3. 依据第1款咨询监管机构时，控制者应向监管机构提供：

(a) 适用时，参与处理的控制者、共同控制者和处理者各自的职责，特别是企业集团内部的处理；

(b) 预期处理的目的和方式；

(c) 依据本条例为保护数据主体权利和自由所提供的措施和保障；

(d) 在适用的情况下，数据保护官的详细联系方式；

(e) the data protection impact assessment provided for in Article 35; and

(f) any other information requested by the supervisory authority.

4. Member States shall consult the supervisory authority during the preparation of a proposal for a legislative measure to be adopted by a national parliament, or of a regulatory measure based on such a legislative measure, which relates to processing.

5. Notwithstanding paragraph 1, Member State law may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health.

Section 4

Data protection officer

Article 37

Designation of the data protection officer

1. The controller and the processor shall designate a data protection officer in any case where:

(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

(b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

(c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

2. A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.

3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.

4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.

5. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.

6. The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.

7. The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.

Article 38

Position of the data protection officer

1. The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

(e) 第35条规定的数据保护影响评估；以及

(f) 监管机构要求的任何其他信息。

4. 成员国在准备由国家议会通过的立法措施提案，或基于该立法措施且与处理相关的监管措施时，应咨询监管机构。

5. 尽管有第1款的规定，成员国法律可要求控制者就其为公共利益执行任务而进行的处理(包括与社会保护和公共卫生相关的处理)咨询监管机构并获得事先授权。

第4节

数据保护官

第37条

数据保护官的指定

1. 控制者和处理者在以下任何情况下应指定一名数据保护官：

(a) 处理由公共机关或机构执行，但行使司法职能的法院除外；(b) 控制者或处理者的核心活动包括因其性质、范围和/或目的而需要对数据主体进行大规模定期和系统性监控的处理操作；或

(c) 控制者或处理者的核心活动包括依据第9条大规模处理特殊类别数据以及第10条所述与刑事定罪和犯罪相关的个人数据。

2. 企业集团可指定一名单一数据保护官，前提是每个场所均可容易地联系到该数据保护官。

3. 当控制者或处理者为公共机关或机构时，可考虑到其组织结构和规模，为多个此类机关或机构指定一名单一数据保护官。

4. 在第1款所述情形以外的情况下，控制者或处理者或代表各类控制者或处理者的协会和其他机构可以或(在联盟或成员国法律要求时)应当指定一名数据保护官。数据保护官可为代表控制者或处理者的此类协会和其他机构行事。

5. 数据保护官应基于专业素质，特别是数据保护法律和实践的专家知识以及履行第39条所述任务的能力来指定。

6. 数据保护官可以是控制者或处理者的工作人员，或基于服务合同履行任务。

7. 控制者或处理者应公布数据保护官的联系方式并将其通报给监管机构。

第38条

数据保护官的职位

1. 控制者和处理者应确保数据保护官适当且及时地参与所有与个人数据保护相关的问题。

2. The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

3. The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.

4. Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.

5. The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.

6. The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

Article 39

Tasks of the data protection officer

1. The data protection officer shall have at least the following tasks:

(a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;

(b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;

(d) to cooperate with the supervisory authority;

(e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

2. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

Section 5

Codes of conduct and certification

Article 40

Codes of conduct

1. The Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.

2. Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to:

(a) fair and transparent processing;

2. 控制者和处理者应通过提供执行第39条所述任务所需的资源以及对个人数据和处理操作的访问权限，并维护其专家知识，来支持数据保护官履行任务。

3. 控制者和处理者应确保数据保护官在行使这些任务方面不接受任何指示。数据保护官不得因履行其任务而被控制者或处理者解雇或处罚。数据保护官应直接向控制者或处理者的最高管理层报告。

4. 数据主体可就与其个人数据处理相关的所有问题以及行使本条例下其权利的事宜联系数据保护官。

5. 数据保护官在履行其任务方面应依据联盟或成员国法律受保密义务的约束。

6. 数据保护官可履行其他任务和职责。控制者或处理者应确保任何此类任务和职责不会导致利益冲突。

第39条

数据保护官的任务

1. 数据保护官至少应承担以下任务：

(a) 告知并建议控制者或处理者以及执行处理的员工其依据本条例及其他联盟或成员国数据保护规定所承担的义务；

(b) 监督对本条例、其他联盟或成员国数据保护规定以及控制者或处理者关于个人数据保护政策的遵守情况，包括职责分配、提高认识和对参与处理操作的工作人员的培训以及相关审计；

(c) 应请求就数据保护影响评估提供建议，并依据Article 35监督其执行；

(d) 与监管机构合作；

(e) 作为监管机构在处理相关问题上的联络点，包括Article 36所述的事先咨询，并在适当情况下就任何其他事项进行咨询。

2. 数据保护官在履行其任务时，应适当考虑与处理操作相关的风险，同时考虑处理的性质、范围、背景和目的。

第5节

行为准则与认证

第40条

行为准则

1. 成员国、监管机构、委员会和欧盟委员会应鼓励制定行为准则，旨在促进本条例的适当适用，同时考虑各处理领域的具体特点以及微型、小型和中型企业的具体需求。

2. 代表各类控制者或处理者的协会和其他机构可编制行为准则，或修订或扩展此类准则，以明确本条例的适用，例如关于：

(a) 公平和透明的处理；

(b) the legitimate interests pursued by controllers in specific contexts;

(c) the collection of personal data;

(d) the pseudonymisation of personal data;

(e) the information provided to the public and to data subjects;

(f) the exercise of the rights of data subjects;

(g) the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained;

(h) the measures and procedures referred to in Articles 24 and 25 and the measures to ensure security of processing referred to in Article 32;

(i) the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects;

(j) the transfer of personal data to third countries or international organisations; or

(k) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79.

3. In addition to adherence by controllers or processors subject to this Regulation, codes of conduct approved pursuant to paragraph 5 of this Article and having general validity pursuant to paragraph 9 of this Article may also be adhered to by controllers or processors that are not subject to this Regulation pursuant to Article 3 in order to provide appropriate safeguards within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (e) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards including with regard to the rights of data subjects.

4. A code of conduct referred to in paragraph 2 of this Article shall contain mechanisms which enable the body referred to in Article 41(1) to carry out the mandatory monitoring of compliance with its provisions by the controllers or processors which undertake to apply it, without prejudice to the tasks and powers of supervisory authorities competent pursuant to Article 55 or 56.

5. Associations and other bodies referred to in paragraph 2 of this Article which intend to prepare a code of conduct or to amend or extend an existing code shall submit the draft code, amendment or extension to the supervisory authority which is competent pursuant to Article 55. The supervisory authority shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation and shall approve that draft code, amendment or extension if it finds that it provides sufficient appropriate safeguards.

6. Where the draft code, or amendment or extension is approved in accordance with paragraph 5, and where the code of conduct concerned does not relate to processing activities in several Member States, the supervisory authority shall register and publish the code.

7. Where a draft code of conduct relates to processing activities in several Member States, the supervisory authority which is competent pursuant to Article 55 shall, before approving the draft code, amendment or extension, submit it in the procedure referred to in Article 63 to the Board which shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation or, in the situation referred to in paragraph 3 of this Article, provides appropriate safeguards.

8. Where the opinion referred to in paragraph 7 confirms that the draft code, amendment or extension complies with this Regulation, or, in the situation referred to in paragraph 3, provides appropriate safeguards, the Board shall submit its opinion to the Commission.

9. The Commission may, by way of implementing acts, decide that the approved code of conduct, amendment or extension submitted to it pursuant to paragraph 8 of this Article have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).

(b) 控制者在特定情境下追求的正当利益；

(c) 个人数据的收集；

(d) 个人数据的假名化；

(e) 向公众和数据主体提供的信息；

(f) 数据主体权利的行使；(g) 向儿童提供的信息及对儿童的保护，以及获取儿童父母责任持有人同意的方式；

(h) Articles 24和25所述的措施和程序，以及Article 32所述的确保处理安全的措施；

(i) 向监管机构通知个人数据泄露以及向数据主体传达此类个人数据泄露；

(j) 向第三国或国际组织传输个人数据；或

(k) 为解决控制者与数据主体之间关于处理的争议而进行的庭外程序和其他争议解决程序，不影响数据主体依据Articles 77和79享有的权利。

3. 除受本条例约束的控制者或处理者遵守外，依据本条第5款批准并依据本条第9款具有普遍效力的行为准则，也可由依据第3条不受本条例约束的控制者或处理者遵守，以便在依据第46(2)条(e)项所述条款向第三国或国际组织传输个人数据的框架内提供适当保障。此类控制者或处理者应通过合同或其他具有法律约束力的文书作出具有约束力和可执行性的承诺，以适用这些适当保障，包括涉及数据主体权利的保障。

4. 本条第2款所述的行为准则应包含相关机制，使Article 41(1)所述的机构能够对承诺适用该准则的控制者或处理者遵守其规定的情况进行强制性监督，不影响依据Article 55或56具有权限的监管机构的任务和权力。

5. 拟制定行为准则或修订、扩展现有行为准则的本条第2款所述协会及其他机构，应向依据Article 55具有管辖权的监管机构提交准则草案、修订或扩展内容。监管机构应就该准则草案、修订或扩展内容是否符合本条例发表意见，如认定其提供了充分适当的保障措施，则应批准该准则草案、修订或扩展内容。

6. 若准则草案、修订或扩展依据第5款获得批准，且相关行为准则不涉及多个成员国的处理活动，监管机构应登记并公布该准则。

7. 行为准则草案涉及多个成员国的处理活动时，依据Article 55具有管辖权的监管机构应在批准该准则草案、修订或扩展内容之前，将其提交至Article 63所述程序中的委员会，委员会应就该准则草案、修订或扩展内容是否符合本条例，或在本条第3款所述情形下是否提供了适当保障措施发表意见。

8. 若第7款所述的意见确认准则草案、修订或扩展符合本条例，或在第3款所述情形下提供了适当保障，委员会应向欧盟委员会提交其意见。

9. 欧盟委员会可通过实施法案决定，依据本条第8款向其提交的已批准行为准则、修订或扩展在联盟内具有普遍效力。该等实施法案应依据Article 93(2)规定的审查程序通过。

10. The Commission shall ensure appropriate publicity for the approved codes which have been decided as having general validity in accordance with paragraph 9.

11. The Board shall collate all approved codes of conduct, amendments and extensions in a register and shall make them publicly available by way of appropriate means.

Article 41

Monitoring of approved codes of conduct

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, the monitoring of compliance with a code of conduct pursuant to Article 40 may be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the competent supervisory authority.

2. A body as referred to in paragraph 1 may be accredited to monitor compliance with a code of conduct where that body has:

(a) demonstrated its independence and expertise in relation to the subject-matter of the code to the satisfaction of the competent supervisory authority;

(b) established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation;

(c) established procedures and structures to handle complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make those procedures and structures transparent to data subjects and the public; and

(d) demonstrated to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.

3. The competent supervisory authority shall submit the draft criteria for accreditation of a body as referred to in paragraph 1 of this Article to the Board pursuant to the consistency mechanism referred to in Article 63.

4. Without prejudice to the tasks and powers of the competent supervisory authority and the provisions of Chapter VIII, a body as referred to in paragraph 1 of this Article shall, subject to appropriate safeguards, take appropriate action in cases of infringement of the code by a controller or processor, including suspension or exclusion of the controller or processor concerned from the code. It shall inform the competent supervisory authority of such actions and the reasons for taking them.

5. The competent supervisory authority shall revoke the accreditation of a body as referred to in paragraph 1 if the conditions for accreditation are not, or are no longer, met or where actions taken by the body infringe this Regulation.

6. This Article shall not apply to processing carried out by public authorities and bodies.

Article 42

Certification

1. The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account.

10. 欧盟委员会应确保依据第9款被认定具有普遍效力的已批准准则得到适当的宣传。

11. 委员会应将所有已批准的行为准则、修订和扩展汇编成册，并通过适当方式使其公开可用。

第41条

对已批准行为准则的监督

1. 不影响主管监管机构依据Articles 57和58的任务和权力，依据Article 40对行为准则遵守情况的监督可由在准则主题事项方面具有适当专业水平并为此目的获得主管监管机构认可的机构进行。

2. 第1款所述的机构在以下情况下可获得认可监督行为准则的遵守情况：

(a) 已向主管监管机构证明其在准则主题事项方面的独立性和专业性，令其满意；

(b) 已建立程序，使其能够评估相关控制者和处理者适用准则的资格，监督其遵守准则规定的情况，并定期审查其运作；

(c) 已建立程序和结构，以处理关于违反准则或控制者或处理者实施或正在实施准则方式的投诉，并使这些程序和结构对数据主体和公众透明；以及

(d) 已向主管监管机构证明其任务和职责不会导致利益冲突，令其满意。

3. 主管监管机构应依据Article 63所述的一致性机制，向委员会提交本条第1款所述机构认可标准的草案。

4. 在不影响主管监管机构的职责和权力以及第八章规定的前提下，本条第1款所述机构应在采取适当保障措施的情况下，在控制者或处理者违反行为准则时采取适当行动，包括暂停或取消相关控制者或处理者参与该准则的资格。该机构应将此类行动及采取行动的理由告知主管监管机构。

5. 若认可条件未满足或不再满足，或该机构采取的行动违反本条例，主管监管机构应撤销对第1款所述机构的认可。

6. 本条不适用于公共当局和机构进行的处理。

第42条

认证

1. 成员国、监管机构、委员会和欧盟委员会应鼓励，特别是在联盟层面，建立数据保护认证机制以及数据保护印章和标记，以证明控制者和处理者的处理操作符合本条例。应考虑微型、小型和中型企业的具体需求。

2. In addition to adherence by controllers or processors subject to this Regulation, data protection certification mechanisms, seals or marks approved pursuant to paragraph 5 of this Article may be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation pursuant to Article 3 within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (f) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards, including with regard to the rights of data subjects.

3. The certification shall be voluntary and available via a process that is transparent.

4. A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the tasks and powers of the supervisory authorities which are competent pursuant to Article 55 or 56.

5. A certification pursuant to this Article shall be issued by the certification bodies referred to in Article 43 or by the competent supervisory authority, on the basis of criteria approved by that competent supervisory authority pursuant to Article 58(3) or by the Board pursuant to Article 63. Where the criteria are approved by the Board, this may result in a common certification, the European Data Protection Seal.

6. The controller or processor which submits its processing to the certification mechanism shall provide the certification body referred to in Article 43, or where applicable, the competent supervisory authority, with all information and access to its processing activities which are necessary to conduct the certification procedure.

7. Certification shall be issued to a controller or processor for a maximum period of three years and may be renewed, under the same conditions, provided that the relevant requirements continue to be met. Certification shall be withdrawn, as applicable, by the certification bodies referred to in Article 43 or by the competent supervisory authority where the requirements for the certification are not or are no longer met.

8. The Board shall collate all certification mechanisms and data protection seals and marks in a register and shall make them publicly available by any appropriate means.

Article 43

Certification bodies

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, certification bodies which have an appropriate level of expertise in relation to data protection shall, after informing the supervisory authority in order to allow it to exercise its powers pursuant to point (h) of Article 58(2) where necessary, issue and renew certification. Member States shall ensure that those certification bodies are accredited by one or both of the following:

(a) the supervisory authority which is competent pursuant to Article 55 or 56;

(b) the national accreditation body named in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council ([1]) in accordance with EN-ISO/IEC 17065/2012 and with the additional requirements established by the supervisory authority which is competent pursuant to Article 55 or 56.

2. Certification bodies referred to in paragraph 1 shall be accredited in accordance with that paragraph only where they have:

(a) demonstrated their independence and expertise in relation to the subject-matter of the certification to the satisfaction of the competent supervisory authority;

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

2. 除受本条例约束的控制者或处理者遵守本条例外，还可设立依据本条第5款批准的数据保护认证机制、印章或标志，用于在依据第46(2)条(f)项所述条款向第三国或国际组织转移个人数据的框架内，证明不受依据第3条约束的控制者或处理者提供了适当保障措施。此类控制者或处理者应通过合同或其他具有法律约束力的文书，作出具有约束力和可强制执行力的承诺，以适用这些适当保障措施，包括涉及数据主体权利的保障措施。

3. 认证应是自愿的，并通过透明的程序提供。

4. 依据本条进行的认证不减轻控制者或处理者遵守本条例的责任，且不影响依据Article 55或56具有管辖权的主管监管机构的任务和权力。

5. 依据本条进行的认证应由Article 43所述认证机构或主管监管机构颁发，其依据是该主管监管机构依据Article 58(3)或委员会依据Article 63批准的标准。标准由委员会批准时，可产生共同认证，即欧洲数据保护印章。

6. 将其处理提交认证机制的控制者或处理者，应向Article 43所述认证机构，或在适用情况下向主管监管机构，提供开展认证程序所必需的一切信息及其处理活动的访问权限。

7. 认证应颁发给控制者或处理者，最长期限为三年，并可在相同条件下续期，前提是相关要求持续得到满足。当认证要求未得到满足或不再得到满足时，认证应视情况由Article 43所述认证机构或主管监管机构撤销。

8. 委员会应将所有认证机制及数据保护印章和标记汇编入登记册，并通过任何适当方式使其公开可获取。

第43条

认证机构

1. 在不影响主管监管机构依据Article 57和58承担的任务和权力的情况下，在数据保护方面具有适当专业水平的认证机构，应在通知监管机构以便其在必要时依据Article 58(2) point (h)行使其权力后，颁发和续期认证。成员国应确保这些认证机构获得下列之一或两者的认可：

(a) 依第55条或第56条具有管辖权的监管机构；

(b) 依据欧洲议会和理事会Regulation (EC) No 765/2008(1)指定、依照EN-ISO/IEC 17065/2012及依据Article 55或56具有管辖权的主管监管机构所确立的附加要求运作的国家认可机构。

2. 第1段所述认证机构只有在具备下列条件时，方应依照该段获得认可：

(a) 已就认证标的向主管监管机构证明其独立性和专业水平，并达到令其满意的程度；

(1) 欧洲议会和理事会2008年7月9日关于产品营销相关认证和市场监督要求并废止第339/93号条例(EEC) 的第765/2008号条例(EC) (OJ L 218, 13.8.2008, p.30)。

(b) undertaken to respect the criteria referred to in Article 42(5) and approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63;

(c) established procedures for the issuing, periodic review and withdrawal of data protection certification, seals and marks;

(d) established procedures and structures to handle complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the controller or processor, and to make those procedures and structures transparent to data subjects and the public; and

(e) demonstrated, to the satisfaction of the competent supervisory authority, that their tasks and duties do not result in a conflict of interests.

3. The accreditation of certification bodies as referred to in paragraphs 1 and 2 of this Article shall take place on the basis of criteria approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63. In the case of accreditation pursuant to point (b) of paragraph 1 of this Article, those requirements shall complement those envisaged in Regulation (EC) No 765/2008 and the technical rules that describe the methods and procedures of the certification bodies.

4. The certification bodies referred to in paragraph 1 shall be responsible for the proper assessment leading to the certification or the withdrawal of such certification without prejudice to the responsibility of the controller or processor for compliance with this Regulation. The accreditation shall be issued for a maximum period of five years and may be renewed on the same conditions provided that the certification body meets the requirements set out in this Article.

5. The certification bodies referred to in paragraph 1 shall provide the competent supervisory authorities with the reasons for granting or withdrawing the requested certification.

6. The requirements referred to in paragraph 3 of this Article and the criteria referred to in Article 42(5) shall be made public by the supervisory authority in an easily accessible form. The supervisory authorities shall also transmit those requirements and criteria to the Board. The Board shall collate all certification mechanisms and data protection seals in a register and shall make them publicly available by any appropriate means.

7. Without prejudice to Chapter VIII, the competent supervisory authority or the national accreditation body shall revoke an accreditation of a certification body pursuant to paragraph 1 of this Article where the conditions for the accreditation are not, or are no longer, met or where actions taken by a certification body infringe this Regulation.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of specifying the requirements to be taken into account for the data protection certification mechanisms referred to in Article 42(1).

9. The Commission may adopt implementing acts laying down technical standards for certification mechanisms and data protection seals and marks, and mechanisms to promote and recognise those certification mechanisms, seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

CHAPTER V

Transfers of personal data to third countries or international organisations

Article 44

General principle for transfers

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.

(b) 已承诺遵守Article 42(5)所述、并经依据Article 55或56具有管辖权的监管机构或委员会依据Article 63批准的标准；

(c) 已建立数据保护认证、印章和标记的颁发、定期审查和撤销程序；

(d) 已建立处理有关违反认证或控制者或处理者实施认证方式(过去或现在)的投诉的程序和架构，并使这些程序和架构对数据主体和公众透明；以及

(e) 已向主管监管机构证明，令其满意，其任务和职责不会导致利益冲突。

3. 本条paragraphs 1 and 2所指的认证机构的认可，应基于依据Article 55或56有管辖权的监管机构或依据Article 63的委员会所批准的标准进行。在依据本条第1款point (b)进行认可的情况下，这些要求应补充Regulation (EC) No 765/2008中所设想的要求以及描述认证机构方法和程序的技术规则。

4. 第1款所述的认证机构应负责进行适当的评估，以促成认证或撤销此类认证，而不影响控制者或处理者遵守本条例的责任。认证的最长期限为五年，在认证机构满足本条所规定要求的前提下，可按相同条件续期。

5. 第1款所述认证机构应向主管监管机构提供授予或撤销所请求认证的理由。

6. 本条第三款所述的要求以及第42(5)条所述的标准，应当由监管机构以易于获取的形式予以公开。监管机构还应当将这些要求和标准转交委员会。委员会应当将所有认证机制和数据保护印章汇编于一份登记册中，并应当通过任何适当方式使其可公开获取。

7. 在不影响第八章的情况下，如认证条件未满足或不再满足，或认证机构采取的行动违反本条例，主管监管机构或国家认证机构应依据本条第1款撤销对认证机构的认可。

8. 应授予委员会权力，依照第92条通过授权法案，以明确第42(1)条所述数据保护认证机制应考虑的要求。

9. 委员会可通过实施法案，规定认证机制和数据保护印章及标志的技术标准，以及促进和承认这些认证机制、印章和标志的机制。这些实施法案应依照第93(2)条所述审查程序通过。

第五章

向第三国或国际组织转移个人数据

第44条

传输的一般原则

任何正在处理中或转移后拟处理至第三国或国际组织的个人数据的转移，仅在控制者和处理者遵守本章规定的条件(包括个人数据从第三国或国际组织 onward transfer 至另一第三国或另一国际组织的情形)且不违反本条例其他规定的情况下，方可进行。本章所有规定均应适用，以确保本条例所保障的自然人保护水平不被削弱。

Article 45

Transfers on the basis of an adequacy decision

1. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:

(a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;

(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and

(c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

3. The Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country, a territory or one or more specified sectors within a third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2 of this Article. The implementing act shall provide for a mechanism for a periodic review, at least every four years, which shall take into account all relevant developments in the third country or international organisation. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority or authorities referred to in point (b) of paragraph 2 of this Article. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 93(2).

4. The Commission shall, on an ongoing basis, monitor developments in third countries and international organisations that could affect the functioning of decisions adopted pursuant to paragraph 3 of this Article and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC.

5. The Commission shall, where available information reveals, in particular following the review referred to in paragraph 3 of this Article, that a third country, a territory or one or more specified sectors within a third country, or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2 of this Article, to the extent necessary, repeal, amend or suspend the decision referred to in paragraph 3 of this Article by means of implementing acts without retro-active effect. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

On duly justified imperative grounds of urgency, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 93(3).

6. The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the decision made pursuant to paragraph 5.

7. A decision pursuant to paragraph 5 of this Article is without prejudice to transfers of personal data to the third country, a territory or one or more specified sectors within that third country, or the international organisation in question pursuant to Articles 46 to 49.

8. The Commission shall publish in the *Official Journal of the European Union* and on its website a list of the third countries, territories and specified sectors within a third country and international organisations for which it has decided that an adequate level of protection is or is no longer ensured.

第45条

基于充分性决定的传输

1. 当委员会已决定第三国、该第三国内的某一领土或一个或多个特定部门，或有关国际组织确保充分保护水平时，可向该第三国或国际组织转移个人数据。此类转移无需任何特别授权。

2. 在评估保护水平的充分性时，委员会应特别考虑以下要素：

(a) 法治、对人权和基本自由的尊重、相关立法(包括一般性和部门性立法，涉及公共安全、国防、国家安全和刑法以及公共当局对个人数据的访问)，以及此类立法、数据保护规则、职业规则和安全措施(包括在该国或国际组织中遵守的将个人数据 onward transfer 至另一第三国或国际组织的规则)的实施情况、判例法，以及数据主体有效的、可强制执行的权利和对个人数据被转移的数据主体有效的行政和司法救济；

(b) 第三国存在一个或多个独立监管机构并有效运作，或国际组织受一个或多个独立监管机构管辖，该机构负责确保和执行数据保护规则的遵守，包括具有充分的执法权力，协助和建议数据主体行使其权利，并与成员国监管机构合作；以及

(c) 有关第三国或国际组织已缔结的国际承诺，或源于具有法律约束力的公约或文书的其他义务，以及其参与多边或区域体系所产生的义务，特别是与个人数据保护有关的义务。

3. 委员会在评估保护水平的充分性后，可通过实施法案决定第三国、第三国境内的一个领土或一个或多个特定部门，或国际组织确保本条第2款含义内的充分保护水平。该实施法案应规定至少每四年进行一次定期审查的机制，该审查应考虑第三国或国际组织的所有相关发展。该实施法案应明确其领土和部门适用范围，并在适用时指明本条第2款point (b)所指的监管机构。该实施法案应按照Article 93(2)所指的审查程序通过。

4. 委员会应持续监测第三国和国际组织的发展动态，这些动态可能影响依据本条第3款通过的决定以及依据指令95/46/EC第25(6)条通过的决定之运作。

5. 在现有信息表明，特别是根据本条第3款所指的审查，第三国、第三国境内的一个领土或一个或多个特定部门，或国际组织不再确保本条第2款含义内的充分保护水平时，委员会应在必要范围内，通过实施法案废除、修订或中止本条第3款所指的决定，且不具追溯效力。该等实施法案应按照Article 93(2)所指的审查程序通过。

在有正当理由的紧急必要情况下，委员会应依照第93(3)条所述程序立即通过适用的实施法案。

6. 委员会应与第三国或国际组织进行磋商，以纠正导致根据第5款作出决定的情况。

7. 依据本条第5款作出的决定不影响依据第46至49条向第三国、该第三国内的某一领土或一个或多个特定部门，或有关国际组织转移个人数据。

8. 委员会应在欧盟官方公报及其网站上公布其已决定确保或不再确保充分保护水平的第三国、领土及第三国内特定部门和国际组织清单。

9. Decisions adopted by the Commission on the basis of Article 25(6) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by a Commission Decision adopted in accordance with paragraph 3 or 5 of this Article.

Article 46

Transfers subject to appropriate safeguards

1. In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:

(a) a legally binding and enforceable instrument between public authorities or bodies;

(b) binding corporate rules in accordance with Article 47;

(c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);

(d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);

(e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or

(f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

3. Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:

(a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or

(b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

4. The supervisory authority shall apply the consistency mechanism referred to in Article 63 in the cases referred to in paragraph 3 of this Article.

5. Authorisations by a Member State or supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed, if necessary, by that supervisory authority. Decisions adopted by the Commission on the basis of Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed, if necessary, by a Commission Decision adopted in accordance with paragraph 2 of this Article.

Article 47

Binding corporate rules

1. The competent supervisory authority shall approve binding corporate rules in accordance with the consistency mechanism set out in Article 63, provided that they:

(a) are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees;

9. 委员会依据指令95/46/EC第25(6)条通过的决定应继续有效，直至被依据本条第3款或第5款通过的委员会决定修订、取代或废止。

第46条

受适当保障措施约束的传输

1. 在未依据第45(3)条作出决定的情况下，控制者或处理者仅在其已提供适当保障，且以数据主体享有可强制执行的数据主体权利和有效法律救济为条件时，方可向第三国或国际组织转移个人数据。

2. 第1款所述适当保障可通过以下方式提供，且无需监管机构的任何特别授权：

(a) 公共机构或机关之间具有法律约束力和可强制执行的文书；

(b) 依照第47条的有约束力的公司规则；(c) 委员会依照第93(2)条所述审查程序通过的标准数据保护条款；

(d) 监管机构通过并经委员会依照第93(2)条所述审查程序批准的标准数据保护条款；

(e) 依照第40条经批准的行为准则，连同第三国控制者或处理者关于适用适当保障(包括涉及数据主体权利方面)的具有约束力和可强制执行的承诺；或

(f) 依照第42条经批准的认证机制，连同第三国控制者或处理者关于适用适当保障(包括涉及数据主体权利方面)的具有约束力和可强制执行的承诺。

3. 在获得主管监管机构授权的前提下，第1款所述适当保障还可特别通过以下方式提供：

(a) 控制者或处理者与第三国或国际组织中的控制者、处理者或个人数据接收方之间的合同条款；或

(b) 拟纳入公共机构或机关之间行政安排的规定，其中包括可强制执行和有效的数据主体权利。

4. 在本条第3款所述情形下，监管机构应适用第63条所述一致性机制。

5. 成员国或监管机构依据指令95/46/EC第26(2)条作出的授权应继续有效，直至该监管机构在必要时予以修订、取代或废止。委员会依据指令95/46/EC第26(4)条通过的决定应继续有效，直至在必要时被依据本条第2款通过的委员会决定修订、取代或废止。

第47条

约束性企业规则

1. 主管监管机构应按照Article 63规定的一致性机制批准有约束力的公司规则，前提是这些规则：

(a) 具有法律约束力，并适用于企业集团或从事联合经济活动的企业集团的每一个相关成员，包括其员工，并由其执行；

(b) expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and

(c) fulfil the requirements laid down in paragraph 2.

2. The binding corporate rules referred to in paragraph 1 shall specify at least:

(a) the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;

(b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;

(c) their legally binding nature, both internally and externally;

(d) the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;

(e) the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with Article 22, the right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States in accordance with Article 79, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;

(f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union; the controller or the processor shall be exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage;

(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in addition to Articles 13 and 14;

(h) the tasks of any data protection officer designated in accordance with Article 37 or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling;

(i) the complaint procedures;

(j) the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred to in point (h) and to the board of the controlling undertaking of a group of undertakings, or of the group of enterprises engaged in a joint economic activity, and should be available upon request to the competent supervisory authority;

(k) the mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority;

(l) the cooperation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority the results of verifications of the measures referred to in point (j);

(m) the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and

(n) the appropriate data protection training to personnel having permanent or regular access to personal data.

(b) 明确赋予数据主体在对其个人数据进行处理方面可强制执行的权利；以及

(c) 满足第2款规定的各项要求。

2. 第1款所指的有约束力的公司规则至少应明确：

(a) 企业集团或从事联合经济活动的企业集团及其每个成员的结构和联系方式；

(b) 数据转移或一系列转移，包括个人数据的类别、处理的类型及其目的、受影响的数据主体类型以及相关第三国的识别；

(c) 其在内外部均具有法律约束力；

(d) 一般数据保护原则的适用，特别是目的限制、数据最小化、有限的存储期限、数据质量、通过设计和默认的数据保护、处理的法律依据、特殊类别的个人数据的处理、确保数据安全的措施，以及关于向不受有约束力的公司规则约束的机构进行后续转移的要求；

(e) 数据主体在处理方面的权利及行使这些权利的方式，包括不受仅基于自动化处理(包括依照Article 22进行的画像)作出的决定约束的权利、依照Article 79向主管监管机构和成员国主管法院提出申诉的权利，以及在违反有约束力的公司规则时获得救济并在适当情况下获得赔偿的权利；

(f) 在成员国境内设立的控制者或处理者接受对任何未在Union设立的相关成员违反有约束力的公司规则的责任；控制者或处理者仅在证明该成员对造成损害的事件不负责任时，方可全部或部分免除该责任；

(g) 除Articles 13和14之外，如何向数据主体提供关于有约束力的公司规则的信息，特别是关于本款points (d)、(e)和(f)所述条款的信息；

(h) 依照Article 37指定的任何数据保护官或负责监督企业集团或从事联合经济活动的企业集团内有约束力的公司规则遵守情况的任何其他人员或实体的任务，以及监督培训和投诉处理；

(i) 投诉程序；

(j) 企业集团或从事联合经济活动的企业集团内部为确保对binding corporate rules遵守情况进行核查的机制。此类机制应包括数据保护审计和确保采取纠正措施以保护data subject权利的方法。此类核查的结果应传达给point (h)所述的个人或实体，以及企业集团或从事联合经济活动的企业集团的控股企业的董事会，并应应competent supervisory authority的要求提供；

(k) 报告和记录规则变更并向监管机构报告这些变更的机制；

(l) 与监管机构的合作机制，以确保企业集团或从事联合经济活动的企业集团的任何成员遵守规则，特别是向监管机构提供对point (j)所述措施的核查结果；

(m) 向主管监管机构报告企业集团或从事联合经济活动的企业集团的成员在第三国所受的任何法律要求(这些要求可能对有约束力的公司规则所提供的保障产生重大不利影响)的机制；以及

(n) 对长期或定期接触个人数据的人员进行适当的数据保护培训。

3. The Commission may specify the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).

Article 48

Transfers or disclosures not authorised by Union law

Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.

Article 49

Derogations for specific situations

1. In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

(a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

(d) the transfer is necessary for important reasons of public interest;

(e) the transfer is necessary for the establishment, exercise or defence of legal claims;

(f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.

2. A transfer pursuant to point (g) of the first subparagraph of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

3. 委员会可规定控制者、处理者和监管机构之间就本Article含义内的有约束力的公司规则交换信息的格式和程序。这些实施法案应按照Article 93(2)规定的审查程序通过。

第48条

未经联盟法律授权的传输或披露

第三国法院或法庭的任何判决和行政当局的任何决定，要求控制者或处理者转移或披露个人数据的，只有在基于请求第三国与Union或成员国之间生效的国际协定(如相互法律协助条约)时，方可被承认或以任何方式强制执行，但不影响依照本章的其他转移依据。

第49条

特定情况下的克减

1. 在缺乏依照Article 45(3)的充分性认定或依照Article 46的适当保障(包括有约束力的公司规则)的情况下，向第三国或国际组织转移或一系列转移个人数据仅可在下列条件之一满足时进行：

(a) 数据主体在被告知由于缺乏充分性认定和适当保障而可能给数据主体带来的此类转移风险后，已明确同意拟议的转移；

(b) 转移对于履行数据主体与控制者之间的合同或实施应数据主体请求采取的合同前措施是必要的；

(c) 转移对于控制者与另一自然人或法人之间为数据主体的利益而订立的合同的订立或履行是必要的；

(d) 该转移对于重要公共利益原因是必要的；

(e) 转移对于确立、行使或抗辩法律主张是必要的；(f) 转移对于保护数据主体或其他人的重大利益是必要的，且数据主体在身体上或法律上无法给予同意；

(g) 转移是从依照Union或成员国法律旨在向公众提供信息且可供公众普遍查阅或可供任何能证明正当利益的人查阅的登记册中作出的，但仅限于在特定情况下满足Union或成员国法律规定的查阅条件。

如果传输不能基于Article 45或46中的规定(包括关于binding corporate rules的规定)，且本款第一项subparagraph所述的针对特定情况的任何derogations均不适用，则只有在传输不具有重复性、仅涉及有限数量的data subject、为controller所追求的强制性的legitimate interests所必需且这些利益不被data subject的利益或权利和自由所超越，并且controller已评估了数据传输的所有相关情况并在此评估基础上就personal data的保护提供了适当保障的情况下，方可向third country或国际组织进行传输。controller应将该传输通知supervisory authority。controller除提供Articles 13和14所述的信息外，还应将传输事宜及所追求的强制性的legitimate interests告知data subject。

2. 依照第1款第一项point (g)进行的转移不得涉及登记册中包含的全部个人数据或全部类别的个人数据。在登记册旨在供具有正当利益的人查阅的情况下，转移仅应应这些人的请求进行，或在他们将成为接收方时进行。

3. Points (a), (b) and (c) of the first subparagraph of paragraph 1 and the second subparagraph thereof shall not apply to activities carried out by public authorities in the exercise of their public powers.

4. The public interest referred to in point (d) of the first subparagraph of paragraph 1 shall be recognised in Union law or in the law of the Member State to which the controller is subject.

5. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation. Member States shall notify such provisions to the Commission.

6. The controller or processor shall document the assessment as well as the suitable safeguards referred to in the second subparagraph of paragraph 1 of this Article in the records referred to in Article 30.

Article 50

International cooperation for the protection of personal data

In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:

(a) develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;

(b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;

(c) engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data;

(d) promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.

CHAPTER VI

Independent supervisory authorities

Section 1

Independent status

Article 51

Supervisory authority

1. Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').

2. Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. For that purpose, the supervisory authorities shall cooperate with each other and the Commission in accordance with Chapter VII.

3. Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which is to represent those authorities in the Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 63.

4. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to this Chapter, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

3. 第1款第一项(a)、(b)和(c)目及其第二项不适用于公共当局在行使其公共权力时开展的活动。

4. 第1款第一项(d)目所指的公共利益应在欧盟法或控制者所受管辖的成员国法律中得到承认。

5. 在缺乏充分性认定的情况下，欧盟法或成员国法律可基于重要的公共利益理由，明确限制向第三国或国际组织转移特定类别的个人数据。成员国应将此类规定通知委员会。

6. 控制者或处理者应将评估以及本条第1款第二项所指的适当保障措施记录在Article 30所指的记录中。

第50条

保护个人数据的国际合作

对于第三国和国际组织，委员会和监管机构应采取适当步骤以：

(a) 发展国际合作机制，以促进个人数据保护立法的有效执行；

(b) 在个人数据保护立法的执行中提供国际互助，包括通过通知、投诉移送、调查协助和信息交换，但须为保护个人数据及其他基本权利和自由采取适当保障措施；

(c) 促使相关利益相关方参与讨论和活动，旨在推进个人数据保护立法执行方面的国际合作；

(d) 促进个人数据保护立法和实践的交流与记录，包括与第三国的管辖权冲突方面。

第六章

独立监管机构

第1节

独立地位

第51条

监管机构

1. 各成员国应设立一个或多个独立的公共机构，负责监督本条例的实施，以保护自然人在处理方面的基本权利和自由，并促进个人数据在欧盟内的自由流动(“监管机构”)。

2. 各监管机构应促进本条例在欧盟范围内的一致适用。为此目的，监管机构应依照Chapter VII相互合作并与委员会合作。

3. 如在一成员国设立多个监管机构，该成员国应指定代表这些机构参加委员会的监管机构，并应规定确保其他机构遵守与Article 63所指一致性机制相关的规则的机制。

4. 各成员国应于25 May 2018前向委员会通知其依据本章通过的法律规定，并应毫不迟延地通知任何影响这些规定的后续修订。

Article 52

Independence

1. Each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation.

2. The member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.

3. Member or members of each supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.

4. Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board.

5. Each Member State shall ensure that each supervisory authority chooses and has its own staff which shall be subject to the exclusive direction of the member or members of the supervisory authority concerned.

6. Each Member State shall ensure that each supervisory authority is subject to financial control which does not affect its independence and that it has separate, public annual budgets, which may be part of the overall state or national budget.

Article 53

General conditions for the members of the supervisory authority

1. Member States shall provide for each member of their supervisory authorities to be appointed by means of a transparent procedure by:

— their parliament;

— their government;

— their head of State; or

— an independent body entrusted with the appointment under Member State law.

2. Each member shall have the qualifications, experience and skills, in particular in the area of the protection of personal data, required to perform its duties and exercise its powers.

3. The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement, in accordance with the law of the Member State concerned.

4. A member shall be dismissed only in cases of serious misconduct or if the member no longer fulfils the conditions required for the performance of the duties.

Article 54

Rules on the establishment of the supervisory authority

1. Each Member State shall provide by law for all of the following:

(a) the establishment of each supervisory authority;

第52条

独立性

1. 各监管机构在依照本条例履行其任务和行使其权力时应完全独立行事。

2. 各监管机构的成员在依照本条例履行其任务和行使其权力时，应不受任何直接或间接的外部影响，且不得寻求或接受任何人的指示。

3. 各监管机构的成员应避免任何与其职责不相容的行为，且在其任期内不得从事任何不相容的职业，无论是否有报酬。

4. 各成员国应确保各监管机构获得有效履行其任务和行使其权力所必需的人力、技术和财政资源、场所和基础设施，包括在互助、合作和参加委员会方面所开展的工作。

5. 各成员国应确保各监管机构选择并拥有自己的工作人员，该工作人员应仅受相关监管机构成员的指导。

6. 各成员国应确保各监管机构接受不影响其独立性的财务控制，并拥有独立的公开年度预算，该预算可构成国家或全国总预算的一部分。

第53条

监管机构成员的一般条件

1. 成员国应规定其各监管机构的成员通过透明程序任命，任命方式为：

- 其议会；

- 其政府；

- 其国家元首；或

- 依据成员国法律受委托进行任命的独立机构。

2. 各成员应具备履行其职责和行使其权力所需的资格、经验和技能，特别是在个人数据保护领域。

3. 成员的职责应在任期届满、辞职或强制退休时终止，依照相关成员国的法律。

4. 成员仅在存在严重不当行为或该成员不再满足履行职责所需条件的情况下方可被解职。

第54条

关于设立监管机构的规定

1. 各成员国应通过法律规定以下所有事项：

(a) 每个监管机构的设立；

(b) the qualifications and eligibility conditions required to be appointed as member of each supervisory authority;

(c) the rules and procedures for the appointment of the member or members of each supervisory authority;

(d) the duration of the term of the member or members of each supervisory authority of no less than four years, except for the first appointment after 24 May 2016, part of which may take place for a shorter period where that is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure;

(e) whether and, if so, for how many terms the member or members of each supervisory authority is eligible for reappointment;

(f) the conditions governing the obligations of the member or members and staff of each supervisory authority, prohibitions on actions, occupations and benefits incompatible therewith during and after the term of office and rules governing the cessation of employment.

2. The member or members and the staff of each supervisory authority shall, in accordance with Union or Member State law, be subject to a duty of professional secrecy both during and after their term of office, with regard to any confidential information which has come to their knowledge in the course of the performance of their tasks or exercise of their powers. During their term of office, that duty of professional secrecy shall in particular apply to reporting by natural persons of infringements of this Regulation.

Section 2

Competence, tasks and powers

Article 55

Competence

1. Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State.

2. Where processing is carried out by public authorities or private bodies acting on the basis of point (c) or (e) of Article 6(1), the supervisory authority of the Member State concerned shall be competent. In such cases Article 56 does not apply.

3. Supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity.

Article 56

Competence of the lead supervisory authority

1. Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.

2. By derogation from paragraph 1, each supervisory authority shall be competent to handle a complaint lodged with it or a possible infringement of this Regulation, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State.

3. In the cases referred to in paragraph 2 of this Article, the supervisory authority shall inform the lead supervisory authority without delay on that matter. Within a period of three weeks after being informed the lead supervisory authority shall decide whether or not it will handle the case in accordance with the procedure provided in Article 60, taking into account whether or not there is an establishment of the controller or processor in the Member State of which the supervisory authority informed it.

(b) 被任命为每个监管机构成员所需的资格和资格条件；

(c) 各监管机构成员的任命规则和程序；(d) 各监管机构成员的任期不少于四年，但24 May 2016之后的首次任命除外，其中部分任命可缩短任期，前提是为通过交错任命程序保护监管机构的独立性而有此必要；

(e) 各监管机构成员是否有资格连任以及如可连任可连任几届；

(f) 各监管机构成员和工作人员的义务条件、任期内及任期后禁止从事的不相容行为、职业和利益，以及有关终止雇佣的规则。

2. 各监管机构的成员及工作人员，在任职期间及任期结束后，均应依照Union或成员国法律，对其在履行任务或行使权力过程中获知的任何机密信息承担职业保密义务。在任职期间，该职业保密义务尤其适用于自然人对违反本条例行为的举报。

第2节

职权、任务与权力

第55条

权限

1. 各监管机构应在其本国成员国领土内有权履行依照本条例分配给它的任务并行使其被授予的权力。

2. 当处理由公共机构或依据Article 6(1)的point (c)或(e)行事的私人机构进行时，相关成员国的监管机构应具有管辖权。在此类情况下，Article 56不适用。

3. 监管机构无权监督法院以司法身份进行的处理操作。

第56条

主导监管机构的权限

1. 在不影响Article 55的情况下，控制者或处理者的主要设立地或单一设立地的监管机构应有权作为主导监管机构，依照Article 60规定的程序，对该控制者或处理者进行的跨境处理采取行动。

2. 作为对paragraph 1的减损，如果标的事项仅涉及其成员国境内的设立地，或实质上仅影响其成员国境内的数据主体，各监管机构应有权处理向其提出的投诉或可能违反本条例的行为。

3. 在本条第2款所述情形下，监管机构应当毫不迟延地将该事项通知主导监管机构。主导监管机构应当在获知后三周内，考虑控制者或处理者在其获知该信息的监管机构所属成员国内是否设有机构，决定是否依照Article 60规定的程序处理该案件。

4. Where the lead supervisory authority decides to handle the case, the procedure provided in Article 60 shall apply. The supervisory authority which informed the lead supervisory authority may submit to the lead supervisory authority a draft for a decision. The lead supervisory authority shall take utmost account of that draft when preparing the draft decision referred to in Article 60(3).

5. Where the lead supervisory authority decides not to handle the case, the supervisory authority which informed the lead supervisory authority shall handle it according to Articles 61 and 62.

6. The lead supervisory authority shall be the sole interlocutor of the controller or processor for the cross-border processing carried out by that controller or processor.

Article 57

Tasks

1. Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:

(a) monitor and enforce the application of this Regulation;

(b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention;

(c) advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing;

(d) promote the awareness of controllers and processors of their obligations under this Regulation;

(e) upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, cooperate with the supervisory authorities in other Member States to that end;

(f) handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;

(g) cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation;

(h) conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority;

(i) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;

(j) adopt standard contractual clauses referred to in Article 28(8) and in point (d) of Article 46(2);

(k) establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 35(4);

(l) give advice on the processing operations referred to in Article 36(2);

(m) encourage the drawing up of codes of conduct pursuant to Article 40(1) and provide an opinion and approve such codes of conduct which provide sufficient safeguards, pursuant to Article 40(5);

(n) encourage the establishment of data protection certification mechanisms and of data protection seals and marks pursuant to Article 42(1), and approve the criteria of certification pursuant to Article 42(5);

(o) where applicable, carry out a periodic review of certifications issued in accordance with Article 42(7);

4. 如果主导监管机构决定处理该案件，应适用Article 60规定的程序。通知主导监管机构的监管机构可以向主导监管机构提交决定草案。主导监管机构在准备Article 60(3)所述的决定草案时，应尽可能考虑该草案。

5. 如果主导监管机构决定不处理该案件，通知主导监管机构的监管机构应依照Articles 61和62处理该案件。

6. 对于控制者或处理者进行的跨境处理，主导监管机构应是该控制者或处理者的唯一对话方。

第57条

任务

1. 在不影响本条例规定的其他任务的情况下，各监管机构应在其领土内：

(a) 监督和执行本条例的适用；(b) 促进公众对处理相关风险、规则、保障措施和权利的认识和理解。专门针对儿童的活动应受到特别关注；

(c) 依照成员国法律，就与处理相关的自然人权利和自由保护有关的立法和行政措施，向国家议会、政府及其他机构和机关提供建议；

(d) 促进控制者和处理者对其在本条例下义务的认识；

(e) 应请求，向任何数据主体提供有关其行使本条例下权利的信息，并在适当情况下为此与其他成员国的监管机构合作；

(f) 处理数据主体或依照Article 80的机构、组织或协会提出的投诉，并在适当范围内调查投诉的标的事项，在合理期限内告知投诉人调查进展和结果，特别是在需要进一步调查或与其他监管机构协调的情况下；

(g) 与其他监管机构合作，包括共享信息和提供互助，以确保本条例的一致适用和执行；

(h) 对本条例的适用进行调查，包括基于从其他监管机构或其他公共机构收到的信息进行调查；

(i) 监测相关发展，只要其对个人数据保护有影响，特别是信息和通信技术及商业实践的发展；

(j) 通过Article 28(8)和Article 46(2)的point (d)所述的标准合同条款；(k) 依照Article 35(4)建立并维护与数据保护影响评估要求相关的清单；

(l) 就Article 36(2)所述的处理操作提供建议；(m) 鼓励依照Article 40(1)制定行为准则，并依照Article 40(5)对提供充分保障的此类行为准则发表意见并予以批准；

(n) 鼓励依照Article 42(1)建立数据保护认证机制及数据保护印章和标记，并依照Article 42(5)批准认证标准；

(o) 在适用情况下，对依照Article 42(7)签发的认证进行定期审查；

(p) draft and publish the criteria for accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;

(q) conduct the accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;

(r) authorise contractual clauses and provisions referred to in Article 46(3);

(s) approve binding corporate rules pursuant to Article 47;

(t) contribute to the activities of the Board;

(u) keep internal records of infringements of this Regulation and of measures taken in accordance with Article 58(2); and

(v) fulfil any other tasks related to the protection of personal data.

2. Each supervisory authority shall facilitate the submission of complaints referred to in point (f) of paragraph 1 by measures such as a complaint submission form which can also be completed electronically, without excluding other means of communication.

3. The performance of the tasks of each supervisory authority shall be free of charge for the data subject and, where applicable, for the data protection officer.

4. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the supervisory authority may charge a reasonable fee based on administrative costs, or refuse to act on the request. The supervisory authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Article 58

Powers

1. Each supervisory authority shall have all of the following investigative powers:

(a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks;

(b) to carry out investigations in the form of data protection audits;

(c) to carry out a review on certifications issued pursuant to Article 42(7);

(d) to notify the controller or the processor of an alleged infringement of this Regulation;

(e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;

(f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.

2. Each supervisory authority shall have all of the following corrective powers:

(a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;

(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;

(c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;

(p) 起草并公布依照Article 41的行为准则监督机构和依照Article 43的认证机构的认可标准；

(q) 对依照Article 41的行为准则监督机构和依照Article 43的认证机构进行认可；

(r) 授权Article 46(3)所述的合同条款和规定；(s) 依照Article 47批准有约束力的公司规则；(t) 为委员会的活动作出贡献；(u) 保存违反本条例的行为及依照Article 58(2)所采取措施的内部记录；以及

(v) 履行与个人数据保护相关的任何其他任务。

2. 各监管机构应通过诸如也可电子填写的投诉提交表格等措施，为提交paragraph 1的point (f)所述投诉提供便利，且不排除其他通信方式。

3. 各监管机构履行任务对数据主体以及(在适用情况下)数据保护官应免费。

4. 如果请求明显无根据或过度，特别是因其具有重复性，监管机构可以收取基于行政成本的合理费用，或拒绝处理该请求。监管机构应承担证明该请求明显无根据或过度的举证责任。

第58条

权力

1. 每个监管机构均应拥有以下所有调查权：

(a) 命令控制者和处理者以及(在适用情况下)控制者或处理者的代表提供其履行职责所需的任何信息；

(b) 以数据保护审计的形式开展调查；

(c) 对依照Article 42(7)签发的认证进行审查；(d) 将涉嫌违反本条例的行为通知控制者或处理者；(e) 从控制者和处理者处获取所有个人数据以及履行职责所需的所有信息；

(f) 依照欧盟法或成员国程序法，进入控制者和处理者的任何场所，包括任何数据处理设备和手段。

2. 每个监管机构均应拥有以下所有纠正权：

(a) 向控制者或处理者发出警告，指出拟进行的处理操作可能违反本条例的规定；

(b) 在处理操作违反本条例规定的情况下，向控制者或处理者发出申诫；

(c) 命令控制者或处理者遵守数据主体根据本条例行使权利的请求；

(d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;

(e) to order the controller to communicate a personal data breach to the data subject;

(f) to impose a temporary or definitive limitation including a ban on processing;

(g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;

(h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;

(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;

(j) to order the suspension of data flows to a recipient in a third country or to an international organisation.

3. Each supervisory authority shall have all of the following authorisation and advisory powers:

(a) to advise the controller in accordance with the prior consultation procedure referred to in Article 36;

(b) to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data;

(c) to authorise processing referred to in Article 36(5), if the law of the Member State requires such prior authorisation;

(d) to issue an opinion and approve draft codes of conduct pursuant to Article 40(5);

(e) to accredit certification bodies pursuant to Article 43;

(f) to issue certifications and approve criteria of certification in accordance with Article 42(5);

(g) to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2);

(h) to authorise contractual clauses referred to in point (a) of Article 46(3);

(i) to authorise administrative arrangements referred to in point (b) of Article 46(3);

(j) to approve binding corporate rules pursuant to Article 47.

4. The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union and Member State law in accordance with the Charter.

5. Each Member State shall provide by law that its supervisory authority shall have the power to bring infringements of this Regulation to the attention of the judicial authorities and where appropriate, to commence or engage otherwise in legal proceedings, in order to enforce the provisions of this Regulation.

6. Each Member State may provide by law that its supervisory authority shall have additional powers to those referred to in paragraphs 1, 2 and 3. The exercise of those powers shall not impair the effective operation of Chapter VII.

Article 59

Activity reports

Each supervisory authority shall draw up an annual report on its activities, which may include a list of types of infringement notified and types of measures taken in accordance with Article 58(2). Those reports shall be transmitted to the national parliament, the government and other authorities as designated by Member State law. They shall be made available to the public, to the Commission and to the Board.

(d) 命令控制者或处理者在适当情况下，以特定方式并在特定期间内使处理操作符合本条例的规定；

(e) 命令控制者向数据主体告知个人数据泄露；

(f) 施加临时性或确定性的限制，包括禁止处理；(g) 命令依照 Article 16、Article 17 和 Article 18 更正或删除个人数据或限制处理，并将此类行动告知依照 Article 17(2) 和 Article 19 已向其披露个人数据的接收方；

(h) 撤销认证或命令认证机构撤销依照 Article 42 和 Article 43 签发的认证，或命令认证机构在认证要求未满足或不再满足时不签发认证；

(i) 依照 Article 83 施加行政罚款，作为本款所述措施的补充或替代，视每个个案的具体情况而定；

(j) 命令暂停向第三国接收方或国际组织的数据流。

3. 每个监管机构均应拥有以下全部授权和咨询权力：(a) 依照 Article 36 所述事先咨询程序向控制者提供建议；(b) 主动或应请求就与个人数据保护相关的任何问题向国家议会、成员国政府或依照成员国法律向其他机构和机关以及公众发表意见；

(c) 在成员国法律要求此类事先授权的情况下，授权Article 36(5)所述的处理；(d) 依照Article 40(5)发表意见并批准行为准则草案；(e) 依照Article 43对认证机构进行认可；(f) 依照Article 42(5)颁发认证并批准认证标准；(g) 通过Article 28(8)和Article 46(2) point(d)所述的标准数据保护条款；(h) 授权Article 46(3) point(a)所述的合同条款；(i) 授权Article 46(3) point(b)所述的行政安排；(j) 依照Article 47批准有约束力的公司规则。

4. 监管机构行使依照本条授予的权力，应遵守欧盟法和成员国法律依照《宪章》规定的适当保障措施，包括有效的司法救济和正当程序。

5. 每个成员国应通过法律规定，其监管机构有权将违反本条例的行为提请司法机关注意，并在适当情况下提起或以其他方式参与法律程序，以执行本条例的规定。

6. 每个成员国可通过法律规定，其监管机构应拥有第 1、2 和 3 款所述权力之外的额外权力。行使这些权力不得损害 Chapter VII 的有效运作。

第59条

活动报告

每个监管机构应就其活动起草年度报告，其中可包括依照 Article 58(2) 所通知的违规类型和所采取措施类型的清单。这些报告应转交国家议会、政府及成员国法律指定的其他机关。报告应向公众、委员会和委员会(Board)提供。

CHAPTER VII

Cooperation and consistency

Section 1

Cooperation

Article 60

Cooperation between the lead supervisory authority and the other supervisory authorities concerned

1. The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavour to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other.

2. The lead supervisory authority may request at any time other supervisory authorities concerned to provide mutual assistance pursuant to Article 61 and may conduct joint operations pursuant to Article 62, in particular for carrying out investigations or for monitoring the implementation of a measure concerning a controller or processor established in another Member State.

3. The lead supervisory authority shall, without delay, communicate the relevant information on the matter to the other supervisory authorities concerned. It shall without delay submit a draft decision to the other supervisory authorities concerned for their opinion and take due account of their views.

4. Where any of the other supervisory authorities concerned within a period of four weeks after having been consulted in accordance with paragraph 3 of this Article, expresses a relevant and reasoned objection to the draft decision, the lead supervisory authority shall, if it does not follow the relevant and reasoned objection or is of the opinion that the objection is not relevant or reasoned, submit the matter to the consistency mechanism referred to in Article 63.

5. Where the lead supervisory authority intends to follow the relevant and reasoned objection made, it shall submit to the other supervisory authorities concerned a revised draft decision for their opinion. That revised draft decision shall be subject to the procedure referred to in paragraph 4 within a period of two weeks.

6. Where none of the other supervisory authorities concerned has objected to the draft decision submitted by the lead supervisory authority within the period referred to in paragraphs 4 and 5, the lead supervisory authority and the supervisory authorities concerned shall be deemed to be in agreement with that draft decision and shall be bound by it.

7. The lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller or processor, as the case may be and inform the other supervisory authorities concerned and the Board of the decision in question, including a summary of the relevant facts and grounds. The supervisory authority with which a complaint has been lodged shall inform the complainant on the decision.

8. By derogation from paragraph 7, where a complaint is dismissed or rejected, the supervisory authority with which the complaint was lodged shall adopt the decision and notify it to the complainant and shall inform the controller thereof.

9. Where the lead supervisory authority and the supervisory authorities concerned agree to dismiss or reject parts of a complaint and to act on other parts of that complaint, a separate decision shall be adopted for each of those parts of the matter. The lead supervisory authority shall adopt the decision for the part concerning actions in relation to the controller, shall notify it to the main establishment or single establishment of the controller or processor on the territory of its Member State and shall inform the complainant thereof, while the supervisory authority of the complainant shall adopt the decision for the part concerning dismissal or rejection of that complaint, and shall notify it to that complainant and shall inform the controller or processor thereof.

10. After being notified of the decision of the lead supervisory authority pursuant to paragraphs 7 and 9, the controller or processor shall take the necessary measures to ensure compliance with the decision as regards processing activities in the context of all its establishments in the Union. The controller or processor shall notify the measures taken for complying with the decision to the lead supervisory authority, which shall inform the other supervisory authorities concerned.

第七章

合作与一致性

第1节

合作

第60条

主导监管机构与其他监管机构之间的合作相关

1. 主导监管机构应依照本条与其他相关监管机构合作，努力达成共识。主导监管机构和相关监管机构应相互交换所有相关信息。

2. 主导监管机构可随时请求其他相关监管机构依照 Article 61 提供互助，并可依照 Article 62 开展联合行动，特别是为开展调查或监测涉及设在另一成员国的控制者或处理者的某项措施的执行情况。

3. 主导监管机构应毫不迟延地将有关事项的相关信息告知其他相关监管机构。其应毫不迟延地向其他相关监管机构提交决定草案以征求其意见，并适当考虑其观点。

4. 其他相关监管机构中任何一方在依照本条第 3 款被咨询后四周内对决定草案提出相关且有理由的异议的，主导监管机构如不采纳该相关且有理由的异议，或认为该异议不相关或无理由，应将事项提交 Article 63 所述一致性机制。

5. 主导监管机构打算采纳所提出的相关且有理由的异议的，应向其他相关监管机构提交修订后的决定草案以征求其意见。该修订后的决定草案应在两周内适用第 4 款所述程序。

6. 其他相关监管机构中无一方在第 4 款和第 5 款所述期间内对主导监管机构提交的决定草案提出异议的，主导监管机构和相关监管机构应被视为同意该决定草案并受其约束。

7. 主导监管机构应通过决定并视情况通知控制者或处理者的主要机构或单一机构，并将该决定告知其他相关监管机构和委员会(Board)，包括相关事实和理由的摘要。已受理投诉的监管机构应将决定告知投诉人。

8. 作为第 7 款的例外，投诉被驳回或拒绝的，已受理投诉的监管机构应通过决定并通知投诉人，且应告知控制者。

9. 主导监管机构与相关监管机构一致同意驳回或拒绝投诉的部分内容并对该投诉的其他部分采取行动的，应当就该事项的每一部分分别作出决定。主导监管机构应当就涉及对控制者采取行动的部分作出决定，将其通知控制者或处理者在其成员国境内的主要机构或单一机构，并告知投诉人；而投诉人所属的监管机构应当就驳回或拒绝该投诉的部分作出决定，将其通知该投诉人，并告知控制者或处理者。

10. 控制者或处理者在依照第 7 款和第 9 款被通知主导监管机构的决定后，应采取必要措施确保其联盟内所有机构的处理活动遵守该决定。控制者或处理者应将为遵守该决定所采取的措施通知主导监管机构，主导监管机构应告知其他相关监管机构。

11. Where, in exceptional circumstances, a supervisory authority concerned has reasons to consider that there is an urgent need to act in order to protect the interests of data subjects, the urgency procedure referred to in Article 66 shall apply.

12. The lead supervisory authority and the other supervisory authorities concerned shall supply the information required under this Article to each other by electronic means, using a standardised format.

Article 61

Mutual assistance

1. Supervisory authorities shall provide each other with relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective cooperation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations.

2. Each supervisory authority shall take all appropriate measures required to reply to a request of another supervisory authority without undue delay and no later than one month after receiving the request. Such measures may include, in particular, the transmission of relevant information on the conduct of an investigation.

3. Requests for assistance shall contain all the necessary information, including the purpose of and reasons for the request. Information exchanged shall be used only for the purpose for which it was requested.

4. The requested supervisory authority shall not refuse to comply with the request unless:

(a) it is not competent for the subject-matter of the request or for the measures it is requested to execute; or

(b) compliance with the request would infringe this Regulation or Union or Member State law to which the supervisory authority receiving the request is subject.

5. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress of the measures taken in order to respond to the request. The requested supervisory authority shall provide reasons for any refusal to comply with a request pursuant to paragraph 4.

6. Requested supervisory authorities shall, as a rule, supply the information requested by other supervisory authorities by electronic means, using a standardised format.

7. Requested supervisory authorities shall not charge a fee for any action taken by them pursuant to a request for mutual assistance. Supervisory authorities may agree on rules to indemnify each other for specific expenditure arising from the provision of mutual assistance in exceptional circumstances.

8. Where a supervisory authority does not provide the information referred to in paragraph 5 of this Article within one month of receiving the request of another supervisory authority, the requesting supervisory authority may adopt a provisional measure on the territory of its Member State in accordance with Article 55(1). In that case, the urgent need to act under Article 66(1) shall be presumed to be met and require an urgent binding decision from the Board pursuant to Article 66(2).

9. The Commission may, by means of implementing acts, specify the format and procedures for mutual assistance referred to in this Article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board, in particular the standardised format referred to in paragraph 6 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

Article 62

Joint operations of supervisory authorities

1. The supervisory authorities shall, where appropriate, conduct joint operations including joint investigations and joint enforcement measures in which members or staff of the supervisory authorities of other Member States are involved.

11. 在特殊情况下，相关监管机构有理由认为存在为保护数据主体利益而急需采取行动的，应适用 Article 66 所述紧急程序。

12. 主导监管机构和其他相关监管机构应使用标准化格式通过电子方式相互提供本条所要求的信息。

第61条

互助

1. 监管机构应相互提供相关信息和互助，以一致的方式实施和适用本条例，并应制定有效措施相互合作。互助应特别涵盖信息请求和监管措施，例如请求进行事先授权和咨询、检查和调查。

2. 各监管机构应采取一切适当措施，无不当延迟地回应另一监管机构的请求，且不得晚于收到请求后一个月。此类措施尤其可包括传送有关调查开展情况的相关信息。

3. 协助请求应包含所有必要信息，包括请求的目的和理由。所交换的信息仅应用于请求所针对的目的。

4. 被请求的监管机构不得拒绝遵从请求，除非：

(a) 其对请求的主题事项或请求其执行的措施不具有管辖权；或(b) 遵从请求将违反本条例或收到请求的监管机构所受约束的欧盟法或成员国法律。

5. 被请求的监管机构应将为回应请求所采取措施的结果，或视情况将进展告知请求的监管机构。被请求的监管机构应说明根据第4款拒绝遵从请求的任何理由。

6. 被请求的监管机构通常应使用标准化格式，通过电子方式提供其他监管机构所请求的信息。

7. 被请求的监管机构不得对其根据相互协助请求所采取的任何行动收取费用。监管机构可就在特殊情况下因提供相互协助而产生的特定支出相互补偿的规则达成一致。

8. 如监管机构在收到另一监管机构请求后一个月内未提供本条第5款所述信息，请求的监管机构可根据Article 55(1)在其成员国领土上采取临时措施。在此情况下，应推定满足Article 66(1)项下采取行动的紧急需要，并要求Board根据Article 66(2)作出紧急有约束力决定。

9. 委员会可通过实施法案，规定本条所述相互协助的格式和程序，以及监管机构之间、监管机构与Board之间通过电子方式交换信息的安排，特别是本条第6款所述标准化格式。该等实施法案应根据Article 93(2)所述审查程序通过。

第62条

监管机构的联合行动

1. 监管机构应酌情开展联合行动，包括其他成员国的监管机构成员或工作人员参与的联合调查和联合执法措施。

2. Where the controller or processor has establishments in several Member States or where a significant number of data subjects in more than one Member State are likely to be substantially affected by processing operations, a supervisory authority of each of those Member States shall have the right to participate in joint operations. The supervisory authority which is competent pursuant to Article 56(1) or (4) shall invite the supervisory authority of each of those Member States to take part in the joint operations and shall respond without delay to the request of a supervisory authority to participate.

3. A supervisory authority may, in accordance with Member State law, and with the seconding supervisory authority's authorisation, confer powers, including investigative powers on the seconding supervisory authority's members or staff involved in joint operations or, in so far as the law of the Member State of the host supervisory authority permits, allow the seconding supervisory authority's members or staff to exercise their investigative powers in accordance with the law of the Member State of the seconding supervisory authority. Such investigative powers may be exercised only under the guidance and in the presence of members or staff of the host supervisory authority. The seconding supervisory authority's members or staff shall be subject to the Member State law of the host supervisory authority.

4. Where, in accordance with paragraph 1, staff of a seconding supervisory authority operate in another Member State, the Member State of the host supervisory authority shall assume responsibility for their actions, including liability, for any damage caused by them during their operations, in accordance with the law of the Member State in whose territory they are operating.

5. The Member State in whose territory the damage was caused shall make good such damage under the conditions applicable to damage caused by its own staff. The Member State of the seconding supervisory authority whose staff has caused damage to any person in the territory of another Member State shall reimburse that other Member State in full any sums it has paid to the persons entitled on their behalf.

6. Without prejudice to the exercise of its rights *vis-à-vis* third parties and with the exception of paragraph 5, each Member State shall refrain, in the case provided for in paragraph 1, from requesting reimbursement from another Member State in relation to damage referred to in paragraph 4.

7. Where a joint operation is intended and a supervisory authority does not, within one month, comply with the obligation laid down in the second sentence of paragraph 2 of this Article, the other supervisory authorities may adopt a provisional measure on the territory of its Member State in accordance with Article 55. In that case, the urgent need to act under Article 66(1) shall be presumed to be met and require an opinion or an urgent binding decision from the Board pursuant to Article 66(2).

Section 2

Consistency

Article 63

Consistency mechanism

In order to contribute to the consistent application of this Regulation throughout the Union, the supervisory authorities shall cooperate with each other and, where relevant, with the Commission, through the consistency mechanism as set out in this Section.

Article 64

Opinion of the Board

1. The Board shall issue an opinion where a competent supervisory authority intends to adopt any of the measures below. To that end, the competent supervisory authority shall communicate the draft decision to the Board, when it:

(a) aims to adopt a list of the processing operations subject to the requirement for a data protection impact assessment pursuant to Article 35(4);

(b) concerns a matter pursuant to Article 40(7) whether a draft code of conduct or an amendment or extension to a code of conduct complies with this Regulation;

2. 控制者或处理者在多个成员国设有机构，或者处理操作可能对多个成员国的大量数据主体产生重大影响的，各该成员国的监管机构均有权参与联合行动。依照Article 56(1) or(4)享有管辖权的监管机构应当邀请各该成员国的监管机构参加联合行动，并应当毫不迟延地对监管机构提出的参与请求作出回应。

3. 监管机构可以根据成员国法律，并在派遣监管机构的授权下，向参与联合行动的派遣监管机构的成员或工作人员授予包括调查权在内的权力，或者在东道监管机构所在成员国法律允许的范围内，允许派遣监管机构的成员或工作人员根据派遣监管机构所在成员国的法律行使调查权。此类调查权只能在东道监管机构的成员或工作人员的指导和在场的情况下行使。派遣监管机构的成员或工作人员应受东道监管机构所在成员国法律的约束。

4. 如根据第1款，派出监管机构的工作人员在另一成员国开展工作，东道监管机构所在成员国应根据其工作人员开展行动所在领土的成员国法律，对这些人员的行动承担责任，包括对其在行动期间造成的任何损害承担责任。

5. 损害发生地所在成员国应按照适用于其自身工作人员造成损害的相同条件赔偿该损害。派出监管机构所在成员国的工作人员如对另一成员国领土内的任何人造成损害，该成员国应全额偿还该另一成员国代其向有权获得赔偿的人支付的任何款项。

6. 在不影响其针对第三方行使权利的情况下，且除第5款外，各成员国在第1款所规定的情形中，不得就第4款所述损害向另一成员国请求偿还。

7. 如果计划进行联合行动，而某一监管机构未在一个月内遵守本条第2款第二句规定的义务，其他监管机构可以根据Article 55在其成员国领土上采取临时措施。在这种情况下，应推定满足Article 66(1)规定的紧急行动需要，并要求Board根据Article 66(2)提供意见或紧急具有约束力的决定。

第2节

一致性

第63条

一致性机制

为促进本条例在欧盟范围内的一致适用，监管机构应通过本节规定的一致性机制相互合作，并在相关情况下与委员会合作。

第64条

Board的意见

1. 主管监管机构拟采取下列任何措施时，Board应发表意见。为此，主管监管机构应在下列情况下将决定草案通报Board:

(a) 旨在根据Article 35(4)通过须进行数据保护影响评估的处理操作清单；

(b) 涉及根据Article 40(7)判断行为准则草案或行为准则的修订或扩展是否符合本条例的事项；

(c) aims to approve the criteria for accreditation of a body pursuant to Article 41(3) or a certification body pursuant to Article 43(3);

(d) aims to determine standard data protection clauses referred to in point (d) of Article 46(2) and in Article 28(8);

(e) aims to authorise contractual clauses referred to in point (a) of Article 46(3); or

(f) aims to approve binding corporate rules within the meaning of Article 47.

2. Any supervisory authority, the Chair of the Board or the Commission may request that any matter of general application or producing effects in more than one Member State be examined by the Board with a view to obtaining an opinion, in particular where a competent supervisory authority does not comply with the obligations for mutual assistance in accordance with Article 61 or for joint operations in accordance with Article 62.

3. In the cases referred to in paragraphs 1 and 2, the Board shall issue an opinion on the matter submitted to it provided that it has not already issued an opinion on the same matter. That opinion shall be adopted within eight weeks by simple majority of the members of the Board. That period may be extended by a further six weeks, taking into account the complexity of the subject matter. Regarding the draft decision referred to in paragraph 1 circulated to the members of the Board in accordance with paragraph 5, a member which has not objected within a reasonable period indicated by the Chair, shall be deemed to be in agreement with the draft decision.

4. Supervisory authorities and the Commission shall, without undue delay, communicate by electronic means to the Board, using a standardised format any relevant information, including as the case may be a summary of the facts, the draft decision, the grounds which make the enactment of such measure necessary, and the views of other supervisory authorities concerned.

5. The Chair of the Board shall, without undue, delay inform by electronic means:

(a) the members of the Board and the Commission of any relevant information which has been communicated to it using a standardised format. The secretariat of the Board shall, where necessary, provide translations of relevant information; and

(b) the supervisory authority referred to, as the case may be, in paragraphs 1 and 2, and the Commission of the opinion and make it public.

6. The competent supervisory authority shall not adopt its draft decision referred to in paragraph 1 within the period referred to in paragraph 3.

7. The supervisory authority referred to in paragraph 1 shall take utmost account of the opinion of the Board and shall, within two weeks after receiving the opinion, communicate to the Chair of the Board by electronic means whether it will maintain or amend its draft decision and, if any, the amended draft decision, using a standardised format.

8. Where the supervisory authority concerned informs the Chair of the Board within the period referred to in paragraph 7 of this Article that it does not intend to follow the opinion of the Board, in whole or in part, providing the relevant grounds, Article 65(1) shall apply.

Article 65

Dispute resolution by the Board

1. In order to ensure the correct and consistent application of this Regulation in individual cases, the Board shall adopt a binding decision in the following cases:

(a) where, in a case referred to in Article 60(4), a supervisory authority concerned has raised a relevant and reasoned objection to a draft decision of the lead authority or the lead authority has rejected such an objection as being not relevant or reasoned. The binding decision shall concern all the matters which are the subject of the relevant and reasoned objection, in particular whether there is an infringement of this Regulation;

(c) 旨在根据Article 41(3)批准机构认证标准，或根据Article 43(3)批准认证机构；

(d) 旨在确定Article 46(2)第(d)点和Article 28(8)所述标准数据保护条款；(e) 旨在授权Article 46(3)第(a)点所述合同条款；或

(f) 旨在批准第47条意义上的约束性企业规则。

2. 任何监管机构、Board主席或委员会均可请求Board审查任何具有普遍适用性或在一个以上成员国产生效果的事项，以获取意见，特别是在主管监管机构未遵守根据Article 61的相互协助义务或根据Article 62的联合行动义务的情况下。

3. 在第1款和第2款所述情况下，Board应就提交给其的事项发表意见，前提是其尚未就同一事项发表意见。该意见应在八周内由Board成员简单多数通过。考虑到主题事项的复杂性，该期限可以再延长六周。关于根据第5款分发给Board成员的第1款所述决定草案，未在主席指明的合理期限内提出异议的成员，应被视为同意该决定草案。

4. 监管机构和委员会应无不当延迟地使用标准化格式通过电子方式向Board通报任何相关信息，包括视情况包括事实摘要、决定草案、使采取此类措施成为必要的理由，以及其他相关监管机构的意见。

5. 董事会主席应通过电子方式及时通知：

(a) 向Board成员和委员会通报使用标准化格式向其传达的任何相关信息。Board秘书处应在必要时提供相关信息的译文；以及

(b) 视情况向第1款和第2款所述监管机构以及委员会通报该意见并予以公布。

6. 主管监管机构不得在第3款所述期间内通过第1款所述决定草案。

7. 第1款所述监管机构应最大程度考虑Board的意见，并应在收到意见后两周内，使用标准化格式通过电子方式向Board主席通报其将维持还是修订决定草案，以及如有修订后的决定草案。

8. 如相关监管机构在本条第7款所述期间内通知Board主席其不打算全部或部分遵循Board的意见，并提供相关理由，则应适用Article 65(1)。

第65条

由委员会解决争议

1. 为确保本条例在个案中的正确和一致适用，Board应在下列情况下通过有约束力决定：

(a) 在Article 60(4)所述案件中，相关监管机构对主导机构的决定草案提出相关且有理由的异议，或主导机构以该异议不相关或无理由为由予以驳回。有约束力决定应涉及相关且有理由的异议所针对的所有事项，特别是是否存在违反本条例的情形；

(b) where there are conflicting views on which of the supervisory authorities concerned is competent for the main establishment;

(c) where a competent supervisory authority does not request the opinion of the Board in the cases referred to in Article 64(1), or does not follow the opinion of the Board issued under Article 64. In that case, any supervisory authority concerned or the Commission may communicate the matter to the Board.

2. The decision referred to in paragraph 1 shall be adopted within one month from the referral of the subject-matter by a two-thirds majority of the members of the Board. That period may be extended by a further month on account of the complexity of the subject-matter. The decision referred to in paragraph 1 shall be reasoned and addressed to the lead supervisory authority and all the supervisory authorities concerned and binding on them.

3. Where the Board has been unable to adopt a decision within the periods referred to in paragraph 2, it shall adopt its decision within two weeks following the expiration of the second month referred to in paragraph 2 by a simple majority of the members of the Board. Where the members of the Board are split, the decision shall by adopted by the vote of its Chair.

4. The supervisory authorities concerned shall not adopt a decision on the subject matter submitted to the Board under paragraph 1 during the periods referred to in paragraphs 2 and 3.

5. The Chair of the Board shall notify, without undue delay, the decision referred to in paragraph 1 to the supervisory authorities concerned. It shall inform the Commission thereof. The decision shall be published on the website of the Board without delay after the supervisory authority has notified the final decision referred to in paragraph 6.

6. The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged shall adopt its final decision on the basis of the decision referred to in paragraph 1 of this Article, without undue delay and at the latest by one month after the Board has notified its decision. The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged, shall inform the Board of the date when its final decision is notified respectively to the controller or the processor and to the data subject. The final decision of the supervisory authorities concerned shall be adopted under the terms of Article 60(7), (8) and (9). The final decision shall refer to the decision referred to in paragraph 1 of this Article and shall specify that the decision referred to in that paragraph will be published on the website of the Board in accordance with paragraph 5 of this Article. The final decision shall attach the decision referred to in paragraph 1 of this Article.

Article 66

Urgency procedure

1. In exceptional circumstances, where a supervisory authority concerned considers that there is an urgent need to act in order to protect the rights and freedoms of data subjects, it may, by way of derogation from the consistency mechanism referred to in Articles 63, 64 and 65 or the procedure referred to in Article 60, immediately adopt provisional measures intended to produce legal effects on its own territory with a specified period of validity which shall not exceed three months. The supervisory authority shall, without delay, communicate those measures and the reasons for adopting them to the other supervisory authorities concerned, to the Board and to the Commission.

2. Where a supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion or an urgent binding decision from the Board, giving reasons for requesting such opinion or decision.

3. Any supervisory authority may request an urgent opinion or an urgent binding decision, as the case may be, from the Board where a competent supervisory authority has not taken an appropriate measure in a situation where there is an urgent need to act, in order to protect the rights and freedoms of data subjects, giving reasons for requesting such opinion or decision, including for the urgent need to act.

4. By derogation from Article 64(3) and Article 65(2), an urgent opinion or an urgent binding decision referred to in paragraphs 2 and 3 of this Article shall be adopted within two weeks by simple majority of the members of the Board.

(b) 对相关监管机构中哪一个对主要营业机构具有管辖权存在相互冲突的意见；

(c) 在Article 64(1)所述情形中，主管监管机构未请求委员会发表意见，或未遵循委员会根据Article 64发表的意见。在此情况下，任何相关监管机构或委员会可将该事项通报委员会。

2. 第1款所述决定应由委员会成员三分之二多数自事项提交之日起一个月内通过。鉴于事项的复杂性，该期限可再延长一个月。第1款所述决定应说明理由，并送达主导监管机构和所有相关监管机构，且对其具有约束力。

3. 委员会未能在第2款所述期限内通过决定的，应由委员会成员简单多数在第2款所述第二个月届满后两周内通过决定。委员会成员意见分歧的，应由主席投票决定。

4. 相关监管机构不得在第2款和第3款所述期限内就根据第1款提交委员会的事项通过决定。

5. 委员会主席应毫不迟延地将第1款所述决定通知相关监管机构。其应告知委员会。该决定应在监管机构通知第6款所述最终决定后毫不迟延地在委员会网站上公布。

6. 主导监管机构或(视情况而定)受理投诉的监管机构应根据本条第1款所述决定，在无不当延迟的情况下，至迟在Board通知其决定后一个月内通过其最终决定。主导监管机构或(视情况而定)受理投诉的监管机构应将分别向控制者或处理者和数据主体通知其最终决定的日期告知Board。有关监管机构的最终决定应根据Article 60(7)、(8)和(9)的条款通过。最终决定应引用本条第1款所述决定，并应指明该款所述决定将根据本条第5款在Board网站上公布。最终决定应附上本条第1款所述决定。

第66条

紧急程序

1. 在特殊情况下，如果有关监管机构认为存在保护数据主体权利和自由的紧急行动需要，其可以通过克减Articles 63、64和65所述一致性机制或Article 60所述程序的方式，立即在其领土上采取旨在产生法律效力的临时措施，有效期不得超过三个月。该监管机构应毫不延迟地将这些措施及采取这些措施的理由告知其他有关监管机构、Board和Commission。

2. 监管机构已根据第1款采取措施并认为需要紧急采取最终措施的，可请求委员会提供紧急意见或紧急具有约束力的决定，并说明请求该意见或决定的理由。

3. 在存在紧急行动需要以保护数据主体的权利和自由的情形下，主管监管机构未采取适当措施的，任何监管机构可请求委员会提供紧急意见或紧急具有约束力的决定(视情况而定)，并说明请求该意见或决定的理由，包括紧急行动需要的理由。

4. 作为对Article 64(3)和Article 65(2)的减损，本条第2款和第3款所述紧急意见或紧急具有约束力的决定应由委员会成员简单多数在两周内通过。

Article 67

Exchange of information

The Commission may adopt implementing acts of general scope in order to specify the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board, in particular the standardised format referred to in Article 64.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

Section 3

European data protection board

Article 68

European Data Protection Board

1. The European Data Protection Board (the 'Board') is hereby established as a body of the Union and shall have legal personality.

2. The Board shall be represented by its Chair.

3. The Board shall be composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor, or their respective representatives.

4. Where in a Member State more than one supervisory authority is responsible for monitoring the application of the provisions pursuant to this Regulation, a joint representative shall be appointed in accordance with that Member State's law.

5. The Commission shall have the right to participate in the activities and meetings of the Board without voting right. The Commission shall designate a representative. The Chair of the Board shall communicate to the Commission the activities of the Board.

6. In the cases referred to in Article 65, the European Data Protection Supervisor shall have voting rights only on decisions which concern principles and rules applicable to the Union institutions, bodies, offices and agencies which correspond in substance to those of this Regulation.

Article 69

Independence

1. The Board shall act independently when performing its tasks or exercising its powers pursuant to Articles 70 and 71.

2. Without prejudice to requests by the Commission referred to in point (b) of Article 70(1) and in Article 70(2), the Board shall, in the performance of its tasks or the exercise of its powers, neither seek nor take instructions from anybody.

Article 70

Tasks of the Board

1. The Board shall ensure the consistent application of this Regulation. To that end, the Board shall, on its own initiative or, where relevant, at the request of the Commission, in particular:

(a) monitor and ensure the correct application of this Regulation in the cases provided for in Articles 64 and 65 without prejudice to the tasks of national supervisory authorities;

第67条

信息交流

委员会可通过具有普遍适用范围的实施法案，以规定监管机构之间以及监管机构与委员会之间通过电子方式交换信息的安排，特别是Article 64所述标准化格式。

该等实施法案应按照Article 93(2)所述审查程序通过。

第3节

欧洲数据保护委员会

第68条

欧洲数据保护委员会

1. 特此设立欧洲数据保护委员会(以下简称"委员会")，作为欧盟机构，并应具有法律人格。

2. 董事会应由其主席代表。

3. 委员会应由每个成员国一名监管机构负责人和欧洲数据保护监督员或其各自的代表组成。

4. 在一个成员国境内，如果有多个监管机构负责监督本条例各项规定的适用，则应依照该成员国的法律指定一名联合代表。

5. 委员会有权参加委员会的活动和会议，但无表决权。委员会应指定一名代表。委员会主席应向委员会通报委员会的活动。

6. 在Article 65所述情形中，欧洲数据保护监督员仅对涉及适用于欧盟机构、机关、办事处和组织的原则和规则的决定享有表决权，该等原则和规则在实质上与本条例的原则和规则相对应。

第69条

独立性

1. 委员会在根据Article 70和Article 71履行其任务或行使其权力时应独立行事。

2. 在不影响委员会根据Article 70(1) point (b)和Article 70(2)提出的请求的情况下，委员会在履行其任务或行使其权力时，不得寻求或接受任何人的指示。

第70条

董事会的任务

1. 委员会应确保本条例的一致适用。为此，委员会应主动或在相关情况下应委员会请求，特别是：

(a) 在不影响国家监管机构任务的情况下，监督并确保本条例在Article 64和Article 65所规定情形中的正确适用；

(b) advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Regulation;

(c) advise the Commission on the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules;

(d) issue guidelines, recommendations, and best practices on procedures for erasing links, copies or replications of personal data from publicly available communication services as referred to in Article 17(2);

(e) examine, on its own initiative, on request of one of its members or on request of the Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best practices in order to encourage consistent application of this Regulation;

(f) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for further specifying the criteria and conditions for decisions based on profiling pursuant to Article 22(2);

(g) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for establishing the personal data breaches and determining the undue delay referred to in Article 33(1) and (2) and for the particular circumstances in which a controller or a processor is required to notify the personal data breach;

(h) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph as to the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of the natural persons referred to in Article 34(1).

(i) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for the purpose of further specifying the criteria and requirements for personal data transfers based on binding corporate rules adhered to by controllers and binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned referred to in Article 47;

(j) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for the purpose of further specifying the criteria and requirements for the personal data transfers on the basis of Article 49(1);

(k) draw up guidelines for supervisory authorities concerning the application of measures referred to in Article 58(1), (2) and (3) and the setting of administrative fines pursuant to Article 83;

(l) review the practical application of the guidelines, recommendations and best practices referred to in points (e) and (f);

(m) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for establishing common procedures for reporting by natural persons of infringements of this Regulation pursuant to Article 54(2);

(n) encourage the drawing-up of codes of conduct and the establishment of data protection certification mechanisms and data protection seals and marks pursuant to Articles 40 and 42;

(o) carry out the accreditation of certification bodies and its periodic review pursuant to Article 43 and maintain a public register of accredited bodies pursuant to Article 43(6) and of the accredited controllers or processors established in third countries pursuant to Article 42(7);

(p) specify the requirements referred to in Article 43(3) with a view to the accreditation of certification bodies under Article 42;

(q) provide the Commission with an opinion on the certification requirements referred to in Article 43(8);

(r) provide the Commission with an opinion on the icons referred to in Article 12(7);

(s) provide the Commission with an opinion for the assessment of the adequacy of the level of protection in a third country or international organisation, including for the assessment whether a third country, a territory or one or more specified sectors within that third country, or an international organisation no longer ensures an adequate level of protection. To that end, the Commission shall provide the Board with all necessary documentation, including correspondence with the government of the third country, with regard to that third country, territory or specified sector, or with the international organisation.

(b) 就与欧盟个人数据保护相关的任何问题向委员会提供建议，包括对本条例的任何拟议修订；

(c) 就控制者、处理者与监管机构之间为有约束力的公司规则交换信息的格式和程序向委员会提供建议；

(d) 就依据 Article 17(2) 从公开可用的通信服务中删除个人数据的链接、副本或复制件的程序，发布指南、建议和最佳实践；

(e) 主动或应其成员之一或委员会的请求，审查涉及本条例适用的任何问题，并发布指南、建议和最佳实践，以鼓励本条例的一致适用；

(f) 依据本款第(e)项发布指南、建议和最佳实践，以进一步明确依据 Article 22(2) 基于画像作出决定的标准和条件；

(g) 依据本款第(e)项发布指南、建议和最佳实践，以认定个人数据泄露并确定 Article 33(1) 和(2) 所称的不当延迟，以及控制者或处理者须通知个人数据泄露的特定情形；

(h) 依据本款第(e)项发布指南、建议和最佳实践，说明个人数据泄露可能对 Article 34(1) 所称自然人的权利和自由造成高风险的情形。

(i) 依据本款第(e)项发布指南、建议和最佳实践，以进一步明确基于控制者遵守的有约束力的公司规则和处理者遵守的有约束力的公司规则进行个人数据传输的标准和要求，以及确保保护 Article 47 所称相关数据主体的个人数据所必需的进一步要求；

(j) 依据本款第(e)项发布指南、建议和最佳实践，以进一步明确基于 Article 49(1) 进行个人数据传输的标准和要求；

(k) 就监管机构适用 Article 58(1)、(2) 和(3) 所称措施以及依据 Article 83 设定行政罚款，为监管机构制定指南；

(l) 审查第(e)项和第(f)项所称指南、建议和最佳实践的实际适用情况；

(m) 依据本款第(e)项发布指南、建议和最佳实践，以确立自然人依据 Article 54(2) 报告违反本条例行为的共同程序；

(n) 鼓励制定行为准则，并依据 Articles 40 和 42 建立数据保护认证机制以及数据保护印章和标记；

(o) 依据 Article 43 对认证机构进行认可及其定期审查，并依据 Article 43(6) 维护获认可机构的公开登记册，以及依据 Article 42(7) 维护在第三国设立的获认可控制者或处理者的公开登记册；

(p) 明确 Article 43(3) 所称要求，以便依据 Article 42 对认证机构进行认可；

(q) 就 Article 43(8) 所称认证要求向委员会提供意见；

(r) 就 Article 12(7) 所称图标向委员会提供意见；

(s) 就第三国或国际组织保护水平的充分性评估向委员会提供意见，包括评估第三国、该第三国境内的某一地区或一个或多个特定行业，或国际组织是否不再确保充分的保护水平。为此，委员会应向委员会提供所有必要文件，包括与该第三国、地区或特定行业有关的、与该第三国政府或该国际组织的往来函件。

(t) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 64(1), on matters submitted pursuant to Article 64(2) and to issue binding decisions pursuant to Article 65, including in cases referred to in Article 66;

(u) promote the cooperation and the effective bilateral and multilateral exchange of information and best practices between the supervisory authorities;

(v) promote common training programmes and facilitate personnel exchanges between the supervisory authorities and, where appropriate, with the supervisory authorities of third countries or with international organisations;

(w) promote the exchange of knowledge and documentation on data protection legislation and practice with data protection supervisory authorities worldwide.

(x) issue opinions on codes of conduct drawn up at Union level pursuant to Article 40(9); and

(y) maintain a publicly accessible electronic register of decisions taken by supervisory authorities and courts on issues handled in the consistency mechanism.

2. Where the Commission requests advice from the Board, it may indicate a time limit, taking into account the urgency of the matter.

3. The Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee referred to in Article 93 and make them public.

4. The Board shall, where appropriate, consult interested parties and give them the opportunity to comment within a reasonable period. The Board shall, without prejudice to Article 76, make the results of the consultation procedure publicly available.

Article 71

Reports

1. The Board shall draw up an annual report regarding the protection of natural persons with regard to processing in the Union and, where relevant, in third countries and international organisations. The report shall be made public and be transmitted to the European Parliament, to the Council and to the Commission.

2. The annual report shall include a review of the practical application of the guidelines, recommendations and best practices referred to in point (l) of Article 70(1) as well as of the binding decisions referred to in Article 65.

Article 72

Procedure

1. The Board shall take decisions by a simple majority of its members, unless otherwise provided for in this Regulation.

2. The Board shall adopt its own rules of procedure by a two-thirds majority of its members and organise its own operational arrangements.

Article 73

Chair

1. The Board shall elect a chair and two deputy chairs from amongst its members by simple majority.

2. The term of office of the Chair and of the deputy chairs shall be five years and be renewable once.

(t) 依据 Article 64(1) 所称一致性机制就监管机构的决定草案发表意见，就依据 Article 64(2) 提交的事项发表意见，并依据 Article 65 作出有约束力的决定，包括在 Article 66 所称情形中；

(u) 促进监管机构之间的合作以及有效的双边和多边信息与最佳实践交流；

(v) 促进共同培训项目，并便利监管机构之间以及酌情与第三国监管机构或国际组织之间的人员交流；

(w) 促进与全球数据保护监管机构就数据保护立法和实践进行知识和文件交流。

(x) 依据 Article 40(9) 就联盟层面制定的行为准则发表意见；以及(y) 维护一个可公开访问的电子登记册，记录监管机构和法院在一致性机制中所处理事项上作出的决定。

2. 委员会向委员会请求建议时，可考虑事项的紧迫性指明期限。

3. 委员会应将其意见、指南、建议和最佳实践转交委员会和 Article 93 所称委员会，并予以公开。

4. 委员会应酌情咨询利益相关方，并给予其在合理期限内发表意见的机会。在不影响 Article 76 的情况下，委员会应公开咨询程序的结果。

第71条

报告

1. 委员会应就联盟内以及酌情在第三国和国际组织中处理个人数据方面对自然人的保护编写年度报告。该报告应予以公开，并转交欧洲议会、理事会和委员会。

2. 年度报告应包括对 Article 70(1) 第(l)项所称指南、建议和最佳实践以及 Article 65 所称有约束力决定的实际适用情况的审查。

第72条

程序

1. 除本条例另有规定外，委员会应以其成员的简单多数作出决定。

2. 委员会应以其成员的三分之二多数通过其议事规则，并安排其自身的运作事宜。

第73条

主席

1. 董事会应从其成员中以简单多数选举一名主席和两名副主席。

2. 主席和副主席的任期为五年，可连任一次。

Article 74

Tasks of the Chair

1. The Chair shall have the following tasks:

(a) to convene the meetings of the Board and prepare its agenda;

(b) to notify decisions adopted by the Board pursuant to Article 65 to the lead supervisory authority and the supervisory authorities concerned;

(c) to ensure the timely performance of the tasks of the Board, in particular in relation to the consistency mechanism referred to in Article 63.

2. The Board shall lay down the allocation of tasks between the Chair and the deputy chairs in its rules of procedure.

Article 75

Secretariat

1. The Board shall have a secretariat, which shall be provided by the European Data Protection Supervisor.

2. The secretariat shall perform its tasks exclusively under the instructions of the Chair of the Board.

3. The staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation shall be subject to separate reporting lines from the staff involved in carrying out tasks conferred on the European Data Protection Supervisor.

4. Where appropriate, the Board and the European Data Protection Supervisor shall establish and publish a Memorandum of Understanding implementing this Article, determining the terms of their cooperation, and applicable to the staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation.

5. The secretariat shall provide analytical, administrative and logistical support to the Board.

6. The secretariat shall be responsible in particular for:

(a) the day-to-day business of the Board;

(b) communication between the members of the Board, its Chair and the Commission;

(c) communication with other institutions and the public;

(d) the use of electronic means for the internal and external communication;

(e) the translation of relevant information;

(f) the preparation and follow-up of the meetings of the Board;

(g) the preparation, drafting and publication of opinions, decisions on the settlement of disputes between supervisory authorities and other texts adopted by the Board.

Article 76

Confidentiality

1. The discussions of the Board shall be confidential where the Board deems it necessary, as provided for in its rules of procedure.

第74条

主席的任务

1. 主席应承担以下任务：

(a) 召集董事会会议并准备其议程；

(b) 将董事会依据Article 65通过的决定通知主导监管机构和相关监管机构；

(c) 确保及时履行董事会的任务，特别是与Article 63所述一致性机制相关的任务。

2. 董事会应在其议事规则中规定主席与副主席之间的任务分配。

第75条

秘书处

1. 董事会应设秘书处，由欧洲数据保护监督员提供。

2. 秘书处应完全按照董事会主席的指示履行其任务。

3. 参与执行本条例赋予董事会任务的欧洲数据保护监督员工作人员，其报告线应与参与执行赋予欧洲数据保护监督员任务的工作人员相分离。

4. 在适当情况下，董事会和欧洲数据保护监督员应制定并公布一份实施本条的谅解备忘录，确定其合作条款，并适用于参与执行本条例赋予董事会任务的欧洲数据保护监督员工作人员。

5. 秘书处应向董事会提供分析、行政和后勤支持。

6. 秘书处尤其应负责：

(a) 委员会的日常工作；(b) 委员会成员、主席与委员会之间的沟通；(c) 与其他机构和公众的沟通；(d) 内部和外部通信使用电子手段；(e) 相关信息的翻译；(f) 委员会会议的筹备和后续工作；(g) 意见、关于解决监管机构之间争议的决定以及委员会通过的其他文本的筹备、起草和发布。

第76条

保密

1. 董事会的讨论在其认为必要时应予保密，如其议事规则所规定。

2. Access to documents submitted to members of the Board, experts and representatives of third parties shall be governed by Regulation (EC) No 1049/2001 of the European Parliament and of the Council [1].

CHAPTER VIII

Remedies, liability and penalties

Article 77

Right to lodge a complaint with a supervisory authority

1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.

2. The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78.

Article 78

Right to an effective judicial remedy against a supervisory authority

1. Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.

2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to a an effective judicial remedy where the supervisory authority which is competent pursuant to Articles 55 and 56 does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged pursuant to Article 77.

3. Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.

4. Where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or a decision of the Board in the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court.

Article 79

Right to an effective judicial remedy against a controller or processor

1. Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.

2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

[1] Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43).

2. 查阅提交给董事会成员、专家和第三方代表的文件，应适用欧洲议会和理事会Regulation(EC) No 1049/2001(1)。

第八章

救济、责任与处罚

第77条

向监管机构提出申诉的权利

1. 在不影响任何其他行政或司法救济的情况下，每个数据主体均有权向监管机构提出申诉，特别是在其惯常居所、工作地点或所指称侵权发生地的成员国，如果数据主体认为与其相关的个人数据处理违反了本条例。

2. 受理申诉的监管机构应将申诉的进展和结果告知申诉人，包括依据Article 78获得司法救济的可能性。

第78条

针对监管机构的有效司法救济权

1. 在不影响任何其他行政或非司法救济的情况下，每个自然人或法人均有权对监管机构针对其作出的具有法律约束力的决定获得有效的司法救济。

2. 在不影响任何其他行政或非司法救济的情况下，每个数据主体均有权获得有效的司法救济，如果依据Articles 55和56具有管辖权的监管机构未处理申诉，或未在三个月内将依据Article 77提出的申诉的进展或结果告知数据主体。

3. 针对监管机构的诉讼应向该监管机构所在成员国的法院提起。

4. 如针对监管机构的决定提起诉讼，而该决定在一致性机制中先有董事会的意见或决定，监管机构应将该意见或决定转交法院。

第79条

针对控制者或处理者获得有效司法救济的权利

1. 在不影响任何可用的行政或非司法救济(包括依据Article 77向监管机构提出申诉的权利)的情况下，每个数据主体在其认为因对其个人数据的处理不符合本条例而导致其在本条例下的权利受到侵害时，均有权获得有效的司法救济。

2. 针对控制者或处理者的诉讼应向该控制者或处理者设有机构的成员国的法院提起。或者，此类诉讼可向数据主体惯常居所所在成员国的法院提起，除非该控制者或处理者是行使公共权力的成员国公共机构。

(1) 欧洲议会和理事会2001年5月30日关于公众获取欧洲议会、理事会和委员会文件的Regulation(EC) No 1049/2001(OJ L 145, 31.5.2001, p.43)。

Article 80

Representation of data subjects

1. The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.

2. Member States may provide that any body, organisation or association referred to in paragraph 1 of this Article, independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority which is competent pursuant to Article 77 and to exercise the rights referred to in Articles 78 and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing.

Article 81

Suspension of proceedings

1. Where a competent court of a Member State has information on proceedings, concerning the same subject matter as regards processing by the same controller or processor, that are pending in a court in another Member State, it shall contact that court in the other Member State to confirm the existence of such proceedings.

2. Where proceedings concerning the same subject matter as regards processing of the same controller or processor are pending in a court in another Member State, any competent court other than the court first seized may suspend its proceedings.

3. Where those proceedings are pending at first instance, any court other than the court first seized may also, on the application of one of the parties, decline jurisdiction if the court first seized has jurisdiction over the actions in question and its law permits the consolidation thereof.

Article 82

Right to compensation and liability

1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

3. A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.

4. Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.

5. Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2.

第80条

数据主体的代理

1. 数据主体有权委托一个根据成员国法律正式成立、具有符合公共利益的法定目标、并在保护数据主体个人数据方面的权利和自由领域积极开展活动的非营利机构、组织或协会，代表其提出投诉，代表其行使第77条、第78条和第79条所述的权利，并在成员国法律有规定的情况下，代表其行使第82条所述的获得赔偿的权利。

2. 成员国可规定，本条第1款所指的任何机构、组织或协会，在独立于数据主体的授权的情况下，有权在该成员国向依据Article 77具有管辖权的监管机构提出投诉，并在其认为数据主体在本条例下的权利因处理而受到侵害时，行使Articles 78和79所指的权利。

第81条

程序中止

1. 当成员国的主管法院获悉另一成员国法院正在审理涉及同一控制者或处理者的相同处理事项的诉讼时，该法院应联系另一成员国的该法院，以确认该等诉讼的存在。

2. 当另一成员国法院正在审理涉及同一控制者或处理者的相同处理事项的诉讼时，除最先受理的法院以外的任何主管法院可中止其诉讼。

3. 当该等诉讼处于一审待决状态时，除最先受理的法院以外的任何法院亦可经一方当事人申请，在最先受理的法院对相关诉讼具有管辖权且其法律允许合并审理的情况下，拒绝行使管辖权。

第82条

获得赔偿的权利与责任

1. 任何因违反本条例而遭受物质或非物质损害的人，有权就所遭受的损害向控制者或处理者获得赔偿。

2. 参与处理的任何控制者应对因违反本条例的处理所造成的损害承担责任。处理者仅在其未遵守本条例中专门针对处理者的义务，或在其行为超出或违背控制者的合法指示时，才对处理所造成的损害承担责任。

3. 控制者或处理者如能证明其以任何方式均不对引起损害的事件负责，则应免除第2款下的责任。

4. 当多个控制者或处理者，或控制者与处理者共同参与同一处理，且根据第2款和第3款对处理所造成的任何损害负有责任时，为确保对数据主体的有效赔偿，每一控制者或处理者应对全部损害承担责任。

5. 当控制者或处理者已根据第4款就所遭受的损害支付全部赔偿时，该控制者或处理者有权按照第2款规定的条件，向参与同一处理的其他控制者或处理者追偿与其损害责任份额相对应的赔偿部分。

6. Court proceedings for exercising the right to receive compensation shall be brought before the courts competent under the law of the Member State referred to in Article 79(2).

Article 83

General conditions for imposing administrative fines

1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

(b) the intentional or negligent character of the infringement;

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

(e) any relevant previous infringements by the controller or processor;

(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(g) the categories of personal data affected by the infringement;

(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

3. If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;

(b) the obligations of the certification body pursuant to Articles 42 and 43;

(c) the obligations of the monitoring body pursuant to Article 41(4).

6. 行使获得赔偿权利的法院诉讼应向依据Article 79(2)所指成员国法律具有管辖权的法院提起。

第83条

实施行政罚款的一般条件

1. 各监管机构应确保，依据本条对第4款、第5款和第6款所指违反本条例的行为所施加的行政罚款，在每一具体案件中均有效、相称且具有威慑力。

2. 行政罚款应根据每一具体案件的情况，与Article 58(2)中points (a)至(h)和(j)所指措施一并施加或替代该等措施。在决定是否施加行政罚款以及确定每一具体案件中行政罚款的金额时，应适当考虑以下各项：

(a) 违法行为的性质、严重程度和持续时间，同时考虑相关处理的性质、范围或目的以及受影响的数据主体数量和其所遭受损害的程度；

(b) 侵权的故意或过失性质；

(c) 控制者或处理者为减轻数据主体所遭受损害而采取的任何行动；(d) 控制者或处理者的责任程度，同时考虑其依据Articles 25和32实施的技术和组织措施；

(e) 控制者或处理者以往的任何相关违规行为；

(f) 与监管机构合作以补救违法行为并减轻违法行为可能产生的不利影响的程度；

(g) 受违规行为影响的个人数据类别；

(h) 监管机构获悉违法行为的方式，特别是控制者或处理者是否通报了该违法行为以及通报的程度；

(i) 此前是否已就同一事项对相关控制者或处理者下令采取Article 58(2)所指措施，以及是否遵守该等措施；

(j) 是否遵守依据Article 40经批准的行为准则或依据Article 42经批准的认证机制；以及

(k) 适用于案件情况的其他任何加重或减轻因素，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。

3. 控制者或处理者故意或过失地就同一或相关联的处理操作违反本条例多项规定的，行政罚款总额不得超过对最严重违法行为所规定的金额。

4. 违反下列规定的行为，应依据第2款处以最高10 000 000 EUR的行政罚款，或对于企业，处以最高相当于上一财政年度全球年总营业额2 %的行政罚款，以较高者为准：

(a) 控制者和处理者依据Articles 8、11、25至39以及42和43承担的义务；

(b) 认证机构依据第42条和第43条承担的义务；

(c) 监测机构依据第41(4)条承担的义务。

5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;

(b) the data subjects' rights pursuant to Articles 12 to 22;

(c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;

(d) any obligations pursuant to Member State law adopted under Chapter IX;

(e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).

6. Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

7. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58(2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

8. The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.

9. Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. Those Member States shall notify to the Commission the provisions of their laws which they adopt pursuant to this paragraph by 25 May 2018 and, without delay, any subsequent amendment law or amendment affecting them.

Article 84

Penalties

1. Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.

2. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

CHAPTER IX

Provisions relating to specific processing situations

Article 85

Processing and freedom of expression and information

1. Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.

5. 违反下列规定的行为，应依据第2款处以最高20 000 000 EUR的行政罚款，或对于企业，处以最高相当于上一财政年度全球年总营业额4 %的行政罚款，以较高者为准：

(a) 处理的基本原则，包括依据Articles 5、6、7和9的同意条件；

(b) 数据主体依据Articles 12至22享有的权利；(c) 依据Articles 44至49向第三国或国际组织的接收方传输个人数据；

(d) 依据第九章通过的成员国法律所规定的任何义务；

(e) 不遵守监管机构依据Article 58(2)作出的命令或对处理的临时或最终限制或对数据流的暂停，或违反Article 58(1)未能提供访问。

6. 不遵守Article 58(2)所指监管机构命令的行为，应依据本条第2款处以最高20 000 000 EUR的行政罚款，或对于企业，处以最高相当于上一财政年度全球年总营业额4 %的行政罚款，以较高者为准。

7. 在不影响监管机构依据Article 58(2)的纠正权力的情况下，各成员国可制定规则，规定是否以及在何种程度上可对设于该成员国的公共当局和机构施加行政罚款。

8. 监管机构行使本条下的权力应遵守依据欧盟法和成员国法律的适当程序保障，包括有效的司法救济和正当程序。

9. 成员国法律体系未规定行政罚款的，本条可如此适用：由主管监管机构启动罚款程序，并由有管辖权的国家法院作出罚款，同时确保这些法律救济有效，并与监管机构所施加的行政罚款具有同等效果。无论如何，所施加的罚款应当有效、相称且具有劝诫性。这些成员国应在2018年5月25日前将其依据本款通过的法律规定通知委员会，并应毫不迟延地通知其后影响这些规定的任何修订法律或修订。

第84条

处罚

1. 成员国应就违反本条例的其他处罚作出规定，特别是对依据 Article 83 不受行政罚款约束的违法行为，并应采取一切必要措施确保其得到实施。此类处罚应有效、相称且具有威慑力。

2. 各成员国应于 25 May 2018 前向委员会通报其依据第 1 款通过的法律规定，并应毫不迟延地通报任何后续影响这些规定的修订。

第九章

涉及特定处理情形的规定

第85条

处理与表达和信息自由

1. 成员国应通过法律协调依据本条例保护个人数据的权利与表达和信息自由的权利，包括为新闻目的以及学术、艺术或文学表达目的的处理。

2. For processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States shall provide for exemptions or derogations from Chapter II (principles), Chapter III (rights of the data subject), Chapter IV (controller and processor), Chapter V (transfer of personal data to third countries or international organisations), Chapter VI (independent supervisory authorities), Chapter VII (cooperation and consistency) and Chapter IX (specific data processing situations) if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.

3. Each Member State shall notify to the Commission the provisions of its law which it has adopted pursuant to paragraph 2 and, without delay, any subsequent amendment law or amendment affecting them.

Article 86

Processing and public access to official documents

Personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with Union or Member State law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data pursuant to this Regulation.

Article 87

Processing of the national identification number

Member States may further determine the specific conditions for the processing of a national identification number or any other identifier of general application. In that case the national identification number or any other identifier of general application shall be used only under appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation.

Article 88

Processing in the context of employment

1. Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

2. Those rules shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place.

3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

Article 89

Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

1. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in

2. 对于为新闻目的或学术、艺术或文学表达目的而进行的处理，如果为了协调个人数据保护权与表达和信息自由确有必要，成员国应规定对第二章(原则)、第三章(数据主体的权利)、第四章(控制者和处理者)、第五章(向第三国或国际组织传输个人数据)、第六章(独立监管机构)、第七章(合作与一致性)和第九章(特定数据处理情形)的豁免或克减。

3. 各成员国应将其依据第 2 款通过的法律规定，以及任何后续修订法律或影响这些规定的修订，毫不迟延地通报委员会。

第86条

官方文件的处理与公众查阅

公共当局或公共机构或为执行公共利益任务而持有官方文件的私人机构所持官方文件中的个人数据，可由该当局或机构依据其受约束的欧盟法或成员国法律予以披露，以便依据本条例协调公众对官方文件的获取与保护个人数据的权利。

第87条

国家识别号码的处理

成员国可进一步确定处理国家识别号码或任何其他通用标识符的具体条件。在此情况下，国家识别号码或任何其他通用标识符仅应在依据本条例对数据主体的权利和自由提供适当保障的情况下使用。

第88条

雇佣背景下的处理

1. 成员国可以通过法律或集体协议，规定更具体的规则，以确保在雇佣背景下处理雇员个人数据时对权利和自由的保护，特别是为了招聘、履行雇佣合同(包括履行法律或集体协议规定的义务)、工作管理、规划和组织、工作场所的平等和多样性、工作中的健康和安全、保护雇主或客户的财产等目的，以及为了个人或集体行使和享有与雇佣相关的权利和福利的目的，以及为了终止雇佣关系的目的。

2. 这些规则应包括适当且具体的措施，以保障数据主体的人格尊严、正当利益和基本权利，尤其应顾及处理的透明、企业集团或从事联合经济活动的企业集团内部的个人数据传输以及工作场所的监控系统。

3. 各成员国应于 25 May 2018 前向委员会通报其依据第 1 款通过的法律规定，并应毫不迟延地通报任何后续影响这些规定的修订。

第89条

与为公共利益存档目的的处理有关的保障和克减，科学或历史研究目的或统计目的

1. 为公共利益存档目的、科学或历史研究目的或统计目的的处理，应依据本条例对数据主体的权利和自由采取适当保障。这些保障应确保技术和组织措施到位，特别是

order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

2. Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

3. Where personal data are processed for archiving purposes in the public interest, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18, 19, 20 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

4. Where processing referred to in paragraphs 2 and 3 serves at the same time another purpose, the derogations shall apply only to processing for the purposes referred to in those paragraphs.

Article 90

Obligations of secrecy

1. Member States may adopt specific rules to set out the powers of the supervisory authorities laid down in points (e) and (f) of Article 58(1) in relation to controllers or processors that are subject, under Union or Member State law or rules established by national competent bodies, to an obligation of professional secrecy or other equivalent obligations of secrecy where this is necessary and proportionate to reconcile the right of the protection of personal data with the obligation of secrecy. Those rules shall apply only with regard to personal data which the controller or processor has received as a result of or has obtained in an activity covered by that obligation of secrecy.

2. Each Member State shall notify to the Commission the rules adopted pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

Article 91

Existing data protection rules of churches and religious associations

1. Where in a Member State, churches and religious associations or communities apply, at the time of entry into force of this Regulation, comprehensive rules relating to the protection of natural persons with regard to processing, such rules may continue to apply, provided that they are brought into line with this Regulation.

2. Churches and religious associations which apply comprehensive rules in accordance with paragraph 1 of this Article shall be subject to the supervision of an independent supervisory authority, which may be specific, provided that it fulfils the conditions laid down in Chapter VI of this Regulation.

CHAPTER X

Delegated acts and implementing acts

Article 92

Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

以确保遵守数据最小化原则。这些措施可包括假名化，前提是这些目的能够以该方式实现。如果这些目的能够通过不允许或不再允许识别数据主体的进一步处理来实现，则应以此方式实现这些目的。

2. 在为科学或历史研究目的或统计目的处理个人数据时，欧盟法或成员国法律可规定对 Articles 15、16、18 和 21 所述权利的克减，但须符合本条第 1 款所述的条件和保障，且以这些权利可能使特定目的无法实现或受到严重损害为限，并且此类克减为实现这些目的所必需。

3. 在为公共利益存档目的处理个人数据时，欧盟法或成员国法律可规定对 Articles 15、16、18、19、20 和 21 所述权利的克减，但须符合本条第 1 款所述的条件和保障，且以这些权利可能使特定目的无法实现或受到严重损害为限，并且此类克减为实现这些目的所必需。

4. 如果第 2 款和第 3 款所述的处理同时服务于另一目的，则克减仅适用于为这些款所述目的进行的处理。

第90条

保密义务

1. 成员国可以制定具体规则，规定第58(1)条(e)项和(f)项中规定的监管机构对控制者或处理者的权力，这些控制者或处理者根据欧盟或成员国法律或国家主管机构制定的规则，负有职业保密义务或其他同等保密义务，且这对于协调个人数据保护权与保密义务确有必要且相称。这些规则仅适用于控制者或处理者因受该保密义务约束的活动而收到或获得的个人数据。

2. 各成员国应于 25 May 2018 前向委员会通报其依据第 1 款通过的规则，并应毫不迟延地通报任何后续影响这些规则的修订。

第91条

教会和宗教协会的现行数据保护规则

1. 如果在一个成员国中，教会和宗教协会或团体在本条例生效时适用关于处理过程中保护自然人的全面规则，则这些规则可继续适用，前提是它们与本条例保持一致。

2. 依据本条第 1 款适用全面规则的教会和宗教协会应接受独立监管机构的监督，该监管机构可以是专门的，前提是其符合本条例 Chapter VI 规定的条件。

第十章

授权法案与实施法案

第92条

授权的行使

1. 授予委员会通过授权法案的权力须符合本条规定的条件。

2. The delegation of power referred to in Article 12(8) and Article 43(8) shall be conferred on the Commission for an indeterminate period of time from 24 May 2016.

3. The delegation of power referred to in Article 12(8) and Article 43(8) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following that of its publication in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

5. A delegated act adopted pursuant to Article 12(8) and Article 43(8) shall enter into force only if no objection has been expressed by either the European Parliament or the Council within a period of three months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by three months at the initiative of the European Parliament or of the Council.

Article 93

Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.

CHAPTER XI

Final provisions

Article 94

Repeal of Directive 95/46/EC

1. Directive 95/46/EC is repealed with effect from 25 May 2018.

2. References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC shall be construed as references to the European Data Protection Board established by this Regulation.

Article 95

Relationship with Directive 2002/58/EC

This Regulation shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.

2. Article 12(8) 和 Article 43(8) 所述权力的授予应自 24 May 2016 起授予委员会，期限不确定。

3. Article 12(8) 和 Article 43(8) 所述权力的授予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授予。该决定应在其于*Official Journal of the European Union*公布之日的次日起生效，或在其指定的较后日期生效。该决定不影响任何已经生效的授权法案的有效性。

4. 委员会一旦通过授权法案，应同时通知欧洲议会和理事会。

5. 依据 Article 12(8) 和 Article 43(8) 通过的授权法案，只有在将该法案通知欧洲议会和理事会后三个月内，欧洲议会或理事会均未提出异议，或者在该期限届满前，欧洲议会和理事会均已告知委员会其不会提出异议的情况下，方可生效。应欧洲议会或理事会的提议，该期限应延长三个月。

第93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 Regulation(EU) No 182/2011 含义内的委员会。

2. 凡提及本款之处，应适用 Regulation(EU) No 182/2011 的 Article 5。

3. 凡提及本款之处，应适用 Regulation(EU) No 182/2011 的 Article 8，并结合其 Article 5。

第十一章

最终条款

第94条

废除第95/46/EC号指令

1. 指令95/46/EC自2018年5月25日起废止。

2. 对已废止指令的提及应解释为对本条例的提及。对依据 Directive 95/46/EC 的 Article 29 设立的个人数据处理保护工作组的提及，应解释为对本条例设立的欧洲数据保护委员会的提及。

第95条

与 Directive 2002/58/EC 的关系

对于在欧盟公共通信网络中提供公开可用电子通信服务相关的处理，凡其事项受 Directive 2002/58/EC 中规定的相同目标的特定义务约束的，本条例不得对自然人或法人施加额外义务。

Article 96

Relationship with previously concluded Agreements

International agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to 24 May 2016, and which comply with Union law as applicable prior to that date, shall remain in force until amended, replaced or revoked.

Article 97

Commission reports

1. By 25 May 2020 and every four years thereafter, the Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council. The reports shall be made public.

2. In the context of the evaluations and reviews referred to in paragraph 1, the Commission shall examine, in particular, the application and functioning of:

(a) Chapter V on the transfer of personal data to third countries or international organisations with particular regard to decisions adopted pursuant to Article 45(3) of this Regulation and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC;

(b) Chapter VII on cooperation and consistency.

3. For the purpose of paragraph 1, the Commission may request information from Member States and supervisory authorities.

4. In carrying out the evaluations and reviews referred to in paragraphs 1 and 2, the Commission shall take into account the positions and findings of the European Parliament, of the Council, and of other relevant bodies or sources.

5. The Commission shall, if necessary, submit appropriate proposals to amend this Regulation, in particular taking into account of developments in information technology and in the light of the state of progress in the information society.

Article 98

Review of other Union legal acts on data protection

The Commission shall, if appropriate, submit legislative proposals with a view to amending other Union legal acts on the protection of personal data, in order to ensure uniform and consistent protection of natural persons with regard to processing. This shall in particular concern the rules relating to the protection of natural persons with regard to processing by Union institutions, bodies, offices and agencies and on the free movement of such data.

Article 99

Entry into force and application

1. This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

2. It shall apply from 25 May 2018.

第96条

与先前缔结协定的关系

成员国在 24 May 2016 之前缔结的、涉及向第三国或国际组织传输个人数据且符合该日期之前适用的欧盟法的国际协定，应继续有效，直至被修订、取代或撤销。

第97条

委员会报告

1. 委员会应于 25 May 2020 前及此后每四年向欧洲议会和理事会提交关于本条例评估和审查的报告。这些报告应予以公开。

2. 在第 1 款所述评估和审查的背景下，委员会应特别审查以下内容的适用和运作：

(a) 关于向第三国或国际组织传输个人数据的 Chapter V，尤其应顾及依据本条例 Article 45(3) 通过的决定以及依据 Directive 95/46/EC 的 Article 25(6) 通过的决定；

(b) 第七章合作与一致性。

3. 就第1款而言，委员会可要求成员国和监管机构提供信息。

4. 在开展第1款和第2款所述评估和审查时，委员会应考虑欧洲议会、理事会以及其他相关机构或来源的立场和结论。

5. 委员会应在必要时提交适当提案以修订本条例，尤其应考虑信息技术的发展以及信息社会的进展状况。

第98条

对其他欧盟数据保护法律行为的审查

委员会应酌情提交立法提案，以修订其他关于个人数据保护的欧盟法律文件，以确保在个人数据处理方面对自然人提供统一和一致的保护。这尤其涉及有关在欧盟机构、机关、办事处和机构处理个人数据方面保护自然人以及此类数据自由流动的规则。

第99条

生效与适用

1. 本条例自其在欧盟官方公报上公布之日后第二十日起生效。

2. 自2018年5月25日起适用。

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 27 April 2016.

For the European Parliament	*For the Council*
The President	*The President*
M. SCHULZ	J.A. HENNIS-PLASSCHAERT

本条例整体具有约束力，并直接适用于所有成员国。

2016年4月27日订于布鲁塞尔。

欧洲议会	理事会
总统	总统
M.SCHULZ	J.A. 亨尼斯-普拉斯哈特

How this file was made

This is a complete Chinese translation of the General Data Protection Regulation (GDPR). Tables, captions, headers, footers and numbering all keep their original positions. Nothing has been cut.

If you have documents of your own

- Contracts, tenders, standards, patents, reports: original layout kept, CNY 0.15/page
- PDF to Word: free up to 100 pages, CNY 0.10/page beyond that
- Scanned or image-only PDFs: OCR to Word, free
- No sign-up, no login: upload and download

Open the address below and try it with your own file:

https://www.ivyivy.com.cn/gdpr-2016-679-zh

On-premise deployment available (subject to model and compliance review)

Machine translation, provided for reading reference only. For professional judgement and compliance citation, please refer to the original English source.

This page is a translator's note; it is not part of the original document.

这份文件是怎么做出来的

本译本是《通用数据保护条例（GDPR）》的中文全译本，共 88 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/gdpr-2016-679-zh

支持私有化部署（需按贵方模型与合规要求评估）

本译本由机器翻译生成，仅供阅读参考；专业技术判断与合规引用，请以英文原文为准。

本页为译制说明，不属于原文件内容。