DIRECTIVES

DIRECTIVE (EU) 2016/680 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 27 April 2016

on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

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(2) 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 Committee of the Regions ([1]),

Acting in accordance with the ordinary legislative procedure ([2]),

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 Directive is intended to contribute to the accomplishment of an area of freedom, security and justice.

(3) 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 personal data to be processed on an unprecedented scale in order to pursue activities such as the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

(4) The free flow of personal data between 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 within the Union and the transfer of such personal data to third countries and international organisations, should be facilitated while ensuring a high level of protection of personal data. Those developments require the building of a strong and more coherent framework for the protection of personal data in the Union, backed by strong enforcement.

(5) Directive 95/46/EC of the European Parliament and of the Council ([3]) applies to all processing of personal data in Member States in both the public and the private sectors. However, it does not apply to the processing of personal data in the course of an activity which falls outside the scope of Community law, such as activities in the areas of judicial cooperation in criminal matters and police cooperation.

([1]) OJ C 391, 18.12.2012, p. 127.
([2]) 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.
([3]) 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).

指令

欧盟议会和理事会2016年4月27日关于保护自然人在主管当局为预防、调查、发现或起诉刑事犯罪或执行刑事处罚而处理个人数据方面的权利以及关于此类数据自由流动的指令（EU）2016/680，以及废除理事会框架决定2008/977/ JHA

欧洲议会与欧盟理事会

根据《欧洲联盟运作条约》特别是其中第16条第2款的规定，以及欧洲委员会的提案，

在将立法草案提交国家议会后，考虑到地区委员会的意见（[1]），

并依照常规立法程序行事（[2]），

鉴于：

(1) 自然人在个人数据处理方面的保护是一项基本权利。《欧洲联盟基本权利宪章》（下称《宪章》）第8条第1款和《欧洲联盟运作条约》（下称《条约》）第16条第1款规定，人人有权保护其个人数据。

(2) 无论国籍或居住地如何，处理自然人个人数据时，其保护原则与规则均应尊重其基本权利与自由，特别是个人数据保护权。本指令旨在促进自由、安全与正义领域的实现。

(3) 技术的迅猛发展与全球化进程，为个人数据保护带来了全新挑战。个人数据的收集与共享规模已呈现爆发式增长。技术手段使得个人数据能够以前所未有的规模进行处理，从而用于预防、调查、侦破或起诉犯罪行为，以及执行刑事处罚等司法活动。

(4) 为有效预防、调查、侦办或起诉犯罪行为、执行刑事处罚，包括防范和应对欧盟境内公共安全威胁，以及向第三国和国际组织传输个人数据，各主管当局之间应促进个人数据的自由流动，同时确保高水平的个人数据保护。这些发展要求欧盟建立一个更强大、更协调的个人数据保护框架，并辅以强有力的执法措施。

(5) 欧洲议会和欧盟理事会第95/46/EC号指令（以下简称“95/46/EC指令”）适用于欧盟成员国公共部门和私营部门的所有个人数据处理活动。但该指令不适用于超出欧盟法律范畴的个人数据处理行为，例如刑事司法合作和警务合作等领域的相关活动。

([1]) OJ C 391, 18.12.2012, p. 127.

(2) 欧洲议会2014年3月12日的立场（尚未在《官方公报》上公布）和理事会2016年4月8日的一读立场（尚未在《官方公报》上公布）。欧洲议会2016年4月14日的立场。

(3) 欧洲议会和欧洲理事会1995年10月24日关于个人数据处理和此类数据自由流动的个人保护的指令95/46/EC（OJ L 281，23.11.1995，第31页）。

(6) Council Framework Decision 2008/977/JHA ([1]) applies in the areas of judicial cooperation in criminal matters and police cooperation. The scope of application of that Framework Decision is limited to the processing of personal data transmitted or made available between Member States.

(7) Ensuring a consistent and high level of protection of the personal data of natural persons and facilitating the exchange of personal data between competent authorities of Members States is crucial in order to ensure effective judicial cooperation in criminal matters and police cooperation. To that end, the level of protection of the rights and freedoms 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, should be equivalent in all Member States. Effective protection of personal data throughout the Union requires the strengthening of the rights of data subjects and of the obligations of those who process personal data, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data in the Member States.

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

(9) On that basis, Regulation (EU) 2016/679 of the European Parliament and of the Council ([2]) lays down general rules to protect natural persons in relation to the processing of personal data and to ensure the free movement of personal data within the Union.

(10) In Declaration No 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation, annexed to the final act of the intergovernmental conference which adopted the Treaty of Lisbon, the conference acknowledged that specific rules on the protection of personal data and the free movement of personal data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 TFEU may prove necessary because of the specific nature of those fields.

(11) It is therefore appropriate for those fields to be addressed by a directive that lays down the specific rules relating to 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, respecting the specific nature of those activities. Such competent authorities may include not only public authorities such as the judicial authorities, the police or other law-enforcement authorities but also any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of this Directive. Where such a body or entity processes personal data for purposes other than for the purposes of this Directive, Regulation (EU) 2016/679 applies. Regulation (EU) 2016/679 therefore applies in cases where a body or entity collects personal data for other purposes and further processes those personal data in order to comply with a legal obligation to which it is subject. For example, for the purposes of investigation detection or prosecution of criminal offences financial institutions retain certain personal data which are processed by them, and provide those personal data only to the competent national authorities in specific cases and in accordance with Member State law. A body or entity which processes personal data on behalf of such authorities within the scope of this Directive should be bound by a contract or other legal act and by the provisions applicable to processors pursuant to this Directive, while the application of Regulation (EU) 2016/679 remains unaffected for the processing of personal data by the processor outside the scope of this Directive.

(12) The activities carried out by the police or other law-enforcement authorities are focused mainly on the prevention, investigation, detection or prosecution of criminal offences, including police activities without prior knowledge if an incident is a criminal offence or not. Such activities can also include the exercise of authority by taking coercive measures such as police activities at demonstrations, major sporting events and riots. They also include maintaining law and order as a task conferred on the police or other law-enforcement authorities where

([1]) Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (OJ L 350, 30.12.2008, p. 60).

([2]) 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) (see page 1 of this Official Journal).

(6) 理事会框架决定2008/977/ JHA（[1]）适用于刑事司法合作和警察合作领域。该框架决定的适用范围仅限于处理成员国之间传输或提供的个人数据。

(7) 为确保刑事司法合作与警务协作的有效开展，必须建立统一且高水平的自然人个人数据保护机制，并促进成员国主管机关之间的数据交换。为此，各成员国在处理个人数据时，为预防、调查、侦办或起诉犯罪行为及执行刑事处罚（包括维护公共安全、防范威胁等目的）所涉及的自然人权利与自由保护标准，应当保持完全一致。要实现欧盟范围内的个人数据有效保护，需强化数据主体的权利、明确数据处理方的义务，同时确保各成员国在数据保护规则的监督与合规性保障方面拥有同等权限。

(8) 第16条第2款 TFEU 规定，欧洲议会和理事会应制定与自然人在个人数据处理方面的保护有关的规则，以及与个人数据自由流动有关的规则。

(9) 在此基础上，欧洲议会和欧盟理事会颁布的第2016/679号条例（EU）（[2]）制定了通用规则，旨在保护自然人在个人数据处理方面的权益，并确保个人数据在欧盟内部的自由流动。

(10) 在《里斯本条约》政府间会议最终文件所附的关于刑事司法合作和警察合作领域个人数据保护的第21号宣言中，会议承认，由于这些领域的特殊性质，可能需要根据第16条 TFEU 制定关于刑事司法合作和警察合作领域个人数据保护和自由流动的具体规则。

(11) 因此，有必要通过一项指令来规范相关领域，该指令应制定具体规则，规定主管当局在为预防、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时，对自然人进行保护的措施，包括防范和预防对公共安全的威胁，同时尊重这些活动的特殊性质。此类主管当局不仅包括司法机关、警察或其他执法机构等公共权力机关，还包括根据成员国法律被授权行使公共权力的任何其他机构或实体。当此类机构或实体为非本指令目的处理个人数据时，应适用《欧盟第2016/679号条例》。因此，当机构或实体为其他目的收集个人数据并进一步处理这些数据以履行其法律义务时，该条例即适用。例如，在调查、侦查或起诉刑事犯罪时，金融机构会保留由其处理的特定个人数据，并仅在特定情况下且依据成员国法律向主管国家机关提供这些个人数据。根据本指令范围代表此类机关处理个人数据的机构或实体，应受合同或其他法律文件约束，并遵循本指令对处理者适用的规定；而处理者在本指令范围外处理个人数据时，仍适用欧盟第2016/679号条例。

(12) 警方及其他执法机构开展的活动主要聚焦于预防、调查、侦破或起诉刑事犯罪，包括在未事先确认某事件是否构成刑事犯罪的情况下实施的警务行动。此类活动还可包括行使职权的行为。

采取强制措施，如在示威、大型体育赛事和骚乱中进行警察活动。还包括将维持法律和秩序作为赋予警察或其他执法当局的任务，其中

(1) 理事会2008年11月27日关于在刑事事项中警察和司法合作框架内处理的个人数据保护的第2008/977/ JHA 号决定（OJ L 350， 30.12.2008 ，第60页）。

(2) 欧盟第2016/679号条例（2016年4月27日颁布）由欧洲议会与欧盟理事会共同制定，旨在规范自然人在个人数据处理方面的权益保护，并保障数据自由流动，同时废止第95/46/EC号指令（即《通用数据保护条例》）（详见本官方公报第1页）。

necessary to safeguard against and prevent threats to public security and to fundamental interests of the society protected by law which may lead to a criminal offence. Member States may entrust competent authorities with other tasks which are not necessarily carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences, including the safeguarding against and the 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 Regulation (EU) 2016/679.

(13) A criminal offence within the meaning of this Directive should be an autonomous concept of Union law as interpreted by the Court of Justice of the European Union (the 'Court of Justice').

(14) Since this Directive should not apply to the processing of personal data in the course of an activity which falls outside the scope of Union law, activities concerning national security, activities of agencies or units dealing with national security issues and the processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the Treaty on European Union (TEU) should not be considered to be activities falling within the scope of this Directive.

(15) In order to ensure the same level of protection for natural persons through legally enforceable rights throughout the Union and to prevent divergences hampering the exchange of personal data between competent authorities, this Directive should provide for harmonised rules for the protection and the free movement of personal data processed 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. The approximation of Member States' laws should not result in any lessening of the personal data protection they afford but should, on the contrary, seek to ensure a high level of protection within the Union. Member States should not be precluded from providing higher safeguards than those established in this Directive for the protection of the rights and freedoms of the data subject with regard to the processing of personal data by competent authorities.

(16) This Directive is without prejudice to the principle of public access to official documents. Under Regulation (EU) 2016/679 personal data in official documents held by a public authority or a public or private body for the performance of a task carried out in the public interest may be disclosed by that 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.

(17) The protection afforded by this Directive should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data.

(18) 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 Directive.

(19) Regulation (EC) No 45/2001 of the European Parliament and of the Council [1] 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 Regulation (EU) 2016/679.

(20) This Directive does not preclude Member States from specifying processing operations and processing procedures in national rules on criminal procedures in relation to the processing of personal data by courts and other judicial authorities, in particular as regards personal data contained in a judicial decision or in records in relation to criminal proceedings.

[1] 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).

为防范和预防可能构成刑事犯罪的公共安全及受法律保护的社会基本利益威胁，成员国可授权主管机关执行其他非刑事犯罪预防、侦查、侦查或起诉任务，包括维护公共安全及防范相关威胁。在此情况下，若个人数据处理涉及欧盟法律范围内的其他用途，则应适用《欧盟第2016/679号条例》。

(13) 本指令所指的刑事犯罪应为欧盟法律中的一个独立概念，该概念由欧洲联盟法院（ ‘欧洲联盟法院9’ ）解释。

(14) 鉴于本指令不适用于欧盟法律范围之外的活动所涉及的个人数据处理，因此涉及国家安全的活动、处理国家安全事务的机构或单位的活动，以及成员国在执行《欧洲联盟条约》（TEU）第五章第二章所规定活动时进行的个人数据处理，均不应被视为本指令的适用范围。

(15) 为确保欧盟境内通过可依法执行的权利为自然人提供同等保护水平，并防止阻碍主管机关间个人数据交换的分歧，本指令应制定统一规则，规范为预防、调查、侦查或起诉刑事犯罪、执行刑事处罚（包括维护公共安全）而处理的个人数据的保护与自由流动。成员国法律的趋同不应削弱其提供的个人数据保护水平，相反应力求在欧盟内部实现高水平保护。成员国在主管机关处理个人数据时，不得被排除在本指令所确立的更高标准之外，以保障数据主体的权利与自由。

(16) 本指令不影响公众查阅官方文件的原则。根据欧盟第2016/679号条例规定，公共机构或公私实体为履行公共利益相关职责而持有的官方文件中个人数据，可依据该机构或实体所适用的欧盟或成员国法律予以披露，以协调公众查阅官方文件的权利与个人数据保护权之间的平衡。

(17) 本指令所提供的保护应适用于自然人，无论其国籍或居住地，均涉及其个人数据的处理。

(18) 为避免造成严重的规避风险，对自然人的保护应当保持技术中立性，不应受制于所采用的技术手段。该保护原则既适用于通过自动化方式处理个人数据的情形，也适用于人工处理的情形——前提是个人数据被包含或拟纳入备案系统。对于未按特定标准结构化编排的文件或文件集及其封面页，不应纳入本指令的适用范围。

(19) 欧盟议会与理事会第45/2001号条例（EC）适用于欧盟各机构、部门及办事机构处理个人数据的行为。相关条例（EC）第45/2001号及其他适用于此类个人数据处理的欧盟法律文件，均须遵循欧盟第2016/679号条例确立的原则与规则进行调整。

(20) 本指令并不妨碍成员国在刑事诉讼相关国家法规中，就法院及其他机构处理个人数据的行为，对具体操作流程和程序作出规定。

司法当局，特别是涉及司法裁决或刑事诉讼记录中所载个人数据的司法当局。

(1) 2000年12月18日欧洲议会和理事会关于保护个人在欧盟机构和个人数据处理方面的个人以及关于此类数据自由流动的第45/2001号条例（EC）（OJ L 8， 12.1.2001 ，第1页）。

(21) The principles of data protection should apply to any information concerning an identified or 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 no longer identifiable.

(22) 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.

(23) Genetic data should be defined as personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or health of that natural person and 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. Considering the complexity and sensitivity of genetic information, there is a great risk of misuse and re-use for various purposes by the controller. Any discrimination based on genetic features should in principle be prohibited.

(24) 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.

(25) All Member States are affiliated to the International Criminal Police Organisation (Interpol). To fulfil its mission, Interpol receives, stores and circulates personal data to assist competent authorities in preventing and combating international crime. It is therefore appropriate to strengthen cooperation between the Union and Interpol by promoting an efficient exchange of personal data whilst ensuring respect for fundamental rights and freedoms regarding the automatic processing of personal data. Where personal data are transferred from the Union to Interpol, and to countries which have delegated members to Interpol, this Directive, in particular the provisions on international transfers, should apply. This Directive should be without prejudice to the specific rules laid down in Council Common Position 2005/69/JHA ([2]) and Council Decision 2007/533/JHA ([3]).

(26) Any processing of personal data must be lawful, fair and transparent in relation to the natural persons concerned, and only processed for specific purposes laid down by law. This does not in itself prevent the law-enforcement authorities from carrying out activities such as covert investigations or video surveillance. Such activities can be done for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the

([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).
([2]) Council Common Position 2005/69/JHA of 24 January 2005 on exchanging certain data with Interpol (OJ L 27, 29.1.2005, p. 61).
([3]) Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ L 205, 7.8.2007, p. 63).

(21) 数据保护原则应适用于任何涉及已识别或可识别自然人的信息。在判定自然人是否可识别时，应当综合考量所有可能被合理使用的识别手段，包括控制者或第三方直接或间接识别该自然人的手段。判断识别手段是否可能被合理使用时，需综合评估所有客观因素，例如识别所需的成本和时间，同时结合数据处理时的技术水平及后续技术发展。因此，数据保护原则不适用于匿名信息，即与已识别或可识别自然人无关的信息，以及通过特定方式匿名化处理后无法识别数据主体的个人数据。

(22) 根据法律义务在执行公务时需要披露个人数据的公共机构（如税务海关部门、金融调查机构、独立行政机构或负责证券市场监管的金融市场监管机构），若依据欧盟或成员国法律为公共利益开展特定调查而获取必要个人数据，则不应被视为数据接收方。公共机构提交的披露请求必须以书面形式提出，且需附具理由说明，且应属偶发性请求，不得涉及整个档案系统或导致档案系统间的关联。这些公共机构处理个人数据时，应根据数据处理目的遵守适用的数据保护法规。

(23) 遗传数据应定义为与自然人遗传或获得性遗传特征相关的个人数据，这些数据能提供关于该自然人生理或健康状况的独特信息，且源于对该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，或源于可获取同等信息的其他元素分析。鉴于遗传信息的复杂性和敏感性，数据控制者存在滥用和为各种目的重复使用该数据的重大风险。原则上，基于遗传特征的任何歧视行为均应被禁止。

(24) 涉及健康领域的个人数据应包含所有反映数据主体健康状况的信息，这些信息需涵盖该主体过去、现在或未来的生理或心理健康状态。具体包括：根据欧洲议会和理事会第2011/24/EU号指令（[1]）在注册或提供医疗服务过程中收集的自然人信息；为健康用途唯一标识自然人的编号、符号或特定标识符；通过身体部位或生物样本检测获得的信息（包括遗传数据和生物样本）；以及与疾病、残疾、患病风险、医疗史、临床治疗或数据主体生理/生物医学状态相关的信息——无论其来源如何，例如来自医生或其他医疗专业人员、医院、医疗器械或体外诊断检测的结果。

(25) 所有成员国都隶属于国际刑事警察组织（刑警组织）。为了完成其使命，刑警组织接收、存储和流通个人数据，以协助主管当局预防和打击国际犯罪。因此，通过促进个人数据的有效交换，同时确保尊重关于个人数据自动处理的基本权利和自由，加强欧盟与刑警组织之间的合作是适当的。当个人数据从欧盟转移到刑警组织，以及转移到已向刑警组织派遣成员的国家时，本指令，特别是关于国际转移的规定，应适用。本指令不应影响理事会共同立场2005/69/ JHA（[2]）和理事会决定2007/533/ JHA（[3]）中制定的具体规则。

(26) 任何个人数据处理都必须依法、公正且透明地对待相关自然人，并且仅限于法律规定的特定用途。但这并不妨碍执法机关开展诸如秘密调查或视频监控等活动。此类活动可为预防、调查、侦破或起诉刑事犯罪而实施，或用于

(1) 欧洲议会和理事会2011年3月9日关于跨境医疗中患者权利适用的第2011/24/EU号指令（《欧盟官方公报》第88期，2011年4月4日，第45页）。
(2) 2005年1月24日关于与国际刑警组织交换某些数据的理事会共同立场2005/69/ JHA（OJ L 27， 29.1.2005 ，第61页）。
(3) 2007年6月12日关于建立、运行和使用第二代申根信息系统（SIS II）的理事会决定2007/533/ JHA（OJ L 205,2007年8月7日，第63页）。

execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, as long as they are laid down by law and constitute a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the natural person concerned. The data protection principle of fair processing is a distinct notion from the right to a fair trial as defined in Article 47 of the Charter and in Article 6 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR). Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of their personal data and how to exercise their rights in relation to the processing. In particular, the specific purposes for which the 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 and relevant for the purposes for which they are processed. It should, in particular, be ensured that the personal data collected are not excessive and not kept longer than is necessary for the purpose for which they are processed. 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 data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Member States should lay down appropriate safeguards for personal data stored for longer periods for archiving in the public interest, scientific, statistical or historical use.

(27) For the prevention, investigation and prosecution of criminal offences, it is necessary for competent authorities to process personal data collected in the context of the prevention, investigation, detection or prosecution of specific criminal offences beyond that context in order to develop an understanding of criminal activities and to make links between different criminal offences detected.

(28) In order to maintain security in relation to processing and to prevent processing in infringement of this Directive, personal data should be processed in a manner that ensures an appropriate level of security and confidentiality, including by preventing unauthorised access to or use of personal data and the equipment used for the processing, and that takes into account available state of the art and technology, the costs of implementation in relation to the risks and the nature of the personal data to be protected.

(29) Personal data should be collected for specified, explicit and legitimate purposes within the scope of this Directive and should not be processed for purposes incompatible with 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. If personal data are processed by the same or another controller for a purpose within the scope of this Directive other than that for which it has been collected, such processing should be permitted under the condition that such processing is authorised in accordance with applicable legal provisions and is necessary for and proportionate to that other purpose.

(30) The principle of accuracy of data should be applied while taking account of the nature and purpose of the processing concerned. In particular in judicial proceedings, statements containing personal data are based on the subjective perception of natural persons and are not always verifiable. Consequently, the requirement of accuracy should not appertain to the accuracy of a statement but merely to the fact that a specific statement has been made.

(31) It is inherent to the processing of personal data in the areas of judicial cooperation in criminal matters and police cooperation that personal data relating to different categories of data subjects are processed. Therefore, a clear distinction should, where applicable and as far as possible, be made between personal data of different categories of data subjects such as: suspects; persons convicted of a criminal offence; victims and other parties, such as witnesses; persons possessing relevant information or contacts; and associates of suspects and convicted criminals. This should not prevent the application of the right of presumption of innocence as guaranteed by the Charter and by the ECHR, as interpreted in the case-law of the Court of Justice and by the European Court of Human Rights respectively.

(32) The competent authorities should ensure that personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available. In order to ensure the protection of natural persons, the accuracy, completeness or the extent to which the personal data are up to date and the reliability of the personal data transmitted or made available, the competent authorities should, as far as possible, add necessary information in all transmissions of personal data.

(33) Where this Directive refers to Member State law, 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

在执行刑事处罚时，包括防范和预防对公共安全的威胁，只要这些措施符合法律规定，并且在充分考虑相关自然人合法权益的前提下，构成民主社会中必要且相称的措施。公平处理原则与《欧洲人权公约》第47条及《欧洲人权公约》第6条所定义的公平审判权是两个不同的概念。自然人应当了解与其个人数据处理相关的风险、规则、保障措施及权利，以及如何行使与数据处理相关的权利。特别需要强调的是，个人数据处理的具体目的应当明确且合法，并在收集个人数据时即予以确定。个人数据应当与其处理目的充分相关且适当。尤其需要确保所收集的个人数据既不过度也不超出处理目的所需的时间范围。只有当其他合理方式无法实现处理目的时，才应处理个人数据。为确保数据不被长期留存，控制方应设定删除或定期审查的时间限制。各成员国应为出于公共利益、科研、统计或历史用途而长期存储的个人数据，制定相应的保护措施。

(27) 为有效预防、侦查和起诉犯罪行为，主管机关需将特定犯罪案件中收集的个人数据延伸至案件之外，以便深入分析犯罪活动特征，并建立不同犯罪案件之间的关联。

(28) 为确保数据处理过程的安全性并防止违反本指令的规定，个人数据的处理方式应确保达到适当的安全性和保密性标准。具体措施包括：防止未经授权访问或使用个人数据及处理设备；同时需充分考虑现有先进技术水平、实施成本与风险之间的平衡关系，以及所保护个人数据的性质特征。

(29) 个人数据的收集必须严格限定在本指令规定的明确且合法的范围内，不得用于与预防、调查、侦查或起诉刑事犯罪行为、执行刑事处罚（包括维护公共安全、防范公共安全威胁等）相冲突的用途。若同一控制者或第三方控制者出于本指令范围内的其他目的处理个人数据（而非其收集目的），则须满足以下条件：该处理行为须依据适用法律规定获得授权，且必须与该其他目的相适应且必要。

(30) 在适用数据准确性原则时，需结合具体处理的性质与目的。特别是在司法程序中，涉及个人数据的陈述往往基于自然人的主观认知，且难以完全核实。因此，准确性要求不应仅适用于陈述内容本身，而应仅限于确认该特定陈述已被作出这一事实。

(31) 在刑事司法合作与警务合作领域处理个人数据时，涉及不同类别数据主体的个人信息处理具有固有属性。因此，应当在适用且尽可能的情况下，对不同类别的数据主体个人信息作出明确区分，例如：嫌疑人、刑事犯罪定罪人员、受害者及其他相关方（如证人）、掌握相关信息或联系方式的人员，以及嫌疑人和定罪罪犯的关联人员。这不应妨碍适用《欧洲人权公约》及《欧洲人权宪章》所保障的无罪推定权——该权利分别由欧洲法院判例法和欧洲人权法院的解释所确立。

(32) 主管部门应确保不传输或提供不准确、不完整或已过期的个人数据。为保障自然人权益，主管部门应尽可能在所有个人数据传输中补充必要信息，以确保数据的准确性、完整性、时效性及可靠性。

(33) 本指令提及成员国法律、法律依据或立法措施时，不必然要求议会通过立法行为，但不影响宪法规定的要求。

order of the Member State concerned. However, such a Member State law, legal basis or legislative measure should be clear and precise and its application foreseeable for those subject to it, as required by the case-law of the Court of Justice and the European Court of Human Rights. Member State law regulating the processing of personal data within the scope of this Directive should specify at least the objectives, the personal data to be processed, the purposes of the processing and procedures for preserving the integrity and confidentiality of personal data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness.

(34) 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, should cover any operation or set of operations which are performed upon personal data or sets of personal data for those purposes, whether by automated means or otherwise, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, alignment or combination, restriction of processing, erasure or destruction. In particular, the rules of this Directive should apply to the transmission of personal data for the purposes of this Directive to a recipient not subject to this Directive. Such a recipient should encompass a natural or legal person, public authority, agency or any other body to which personal data are lawfully disclosed by the competent authority. Where personal data were initially collected by a competent authority for one of the purposes of this Directive, Regulation (EU) 2016/679 should apply to the processing of those data for purposes other than the purposes of this Directive where such processing is authorised by Union or Member State law. In particular, the rules of Regulation (EU) 2016/679 should apply to the transmission of personal data for purposes outside the scope of this Directive. For the processing of personal data by a recipient that is not a competent authority or that is not acting as such within the meaning of this Directive and to which personal data are lawfully disclosed by a competent authority, Regulation (EU) 2016/679 should apply. While implementing this Directive, Member States should also be able to further specify the application of the rules of Regulation (EU) 2016/679, subject to the conditions set out therein.

(35) In order to be lawful, the processing of personal data under this Directive should be necessary for the performance of a task carried out in the public interest by a competent authority based on Union or Member State law 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. Those activities should cover the protection of vital interests of the data subject. The performance of the tasks of preventing, investigating, detecting or prosecuting criminal offences institutionally conferred by law to the competent authorities allows them to require or order natural persons to comply with requests made. In such a case, the consent of the data subject, as defined in Regulation (EU) 2016/679, should not provide a legal ground for processing personal data by competent authorities. Where the data subject is required to comply with a legal obligation, the data subject has no genuine and free choice, so that the reaction of the data subject could not be considered to be a freely given indication of his or her wishes. This should not preclude Member States from providing, by law, that the data subject may agree to the processing of his or her personal data for the purposes of this Directive, such as DNA tests in criminal investigations or the monitoring of his or her location with electronic tags for the execution of criminal penalties.

(36) Member States should provide that where Union or Member State law applicable to the transmitting competent authority provides for specific conditions applicable in specific circumstances to the processing of personal data, such as the use of handling codes, the transmitting competent authority should inform the recipient of such personal data of those conditions and the requirement to respect them. Such conditions could, for example, include a prohibition against transmitting the personal data further to others, or using them for purposes other than those for which they were transmitted to the recipient, or informing the data subject in the case of a limitation of the right of information without the prior approval of the transmitting competent authority. Those obligations should also apply to transfers by the transmitting competent authority to recipients in third countries or international organisations. Member States should ensure that the transmitting competent authority does not apply such conditions to recipients in other Member States or to agencies, offices and bodies established pursuant to Chapters 4 and 5 of Title V of the TFEU other than those applicable to similar data transmissions within the Member State of that competent authority.

(37) 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 Directive does not imply an acceptance by the Union of theories which attempt

相关成员国的法律体系应当清晰明确。根据欧洲法院和欧洲人权法院的判例法要求，此类成员国法律、法律依据或立法措施必须对适用对象具有可预见性。在本指令适用范围内规范个人数据处理的成员国法律，至少应明确以下内容：处理目的、拟处理的个人数据、处理目的及保护个人数据完整性和保密性的程序，以及数据销毁程序，从而为防范滥用和任意处理风险提供充分保障。

(34) 主管机关为预防、调查、侦查或起诉刑事犯罪行为，或执行刑事处罚（包括维护公共安全及防范公共安全威胁）而处理个人数据时，应涵盖为实现上述目的而对个人数据或个人数据集实施的任何操作或操作组合，无论采用自动化手段或其他方式，例如收集、记录、组织、结构化、存储、调整或修改、检索、查阅、使用、比对或组合、限制处理、删除或销毁。特别地，本指令的规则应适用于将个人数据传输至不受本指令约束的接收方。此类接收方应包括自然人或法人、公共机构、代理机构或任何其他依法获得主管机关合法披露个人数据的实体。当主管机关最初为本指令所列目的收集个人数据时，若该数据处理行为获得欧盟或成员国法律授权，则在处理目的超出本指令规定范围时，应适用《欧盟第2016/679号条例》。特别需要指出的是，该条例规则同样适用于超出本指令范围的个人数据传输行为。对于非主管机关或未按本指令定义行事的接收方处理个人数据的情况——即主管机关依法向其披露个人数据时，也应适用《欧盟第2016/679号条例》。在实施本指令过程中，各成员国可根据条例中规定的条件，进一步明确《欧盟第2016/679号条例》的具体适用范围。

(35) 根据本指令规定，个人数据处理必须符合法律规定，且需基于欧盟或成员国法律，由主管机关为公共利益执行任务所必需。这些任务旨在预防、调查、侦查或起诉刑事犯罪，或执行刑事处罚，包括维护公共安全、防范威胁等。相关活动应涵盖对数据主体核心权益的保护。主管机关依法获得的预防、调查、侦查或起诉刑事犯罪的法定职责，使其有权要求或命令自然人遵守其提出的要求。在此情况下，根据欧盟第2016/679号条例定义的数据主体同意，不应成为主管机关处理个人数据的法律依据。当数据主体被要求履行法律义务时，其缺乏真实自由的选择权，因此其反应不能被视为对其意愿的自由表达。这不应妨碍成员国通过立法规定，数据主体可同意为本指令目的处理其个人数据，例如在刑事调查中进行DNA检测，或通过电子标签监测其行踪以执行刑事处罚。

(36) 成员国应当规定：若欧盟或成员国法律对传输主管机关在特定情况下处理个人数据（例如使用处理代码）有具体规定，传输主管机关应向接收方告知这些规定及遵守要求。此类规定可包括禁止将个人数据进一步传输给第三方、禁止将数据用于接收方授权用途之外的其他目的，或在未经传输主管机关事先批准的情况下限制数据主体知情权。上述义务同样适用于传输主管机关向第三国或国际组织接收方进行的数据传输。成员国应确保发送主管当局不将此类条件适用于其他成员国的接收方或根据 TFEU 第五章第4章和第5章设立的机构、办公室和机构，但适用于该主管当局成员国内的类似数据传输的条件除外。

(37) 根据本指令规定，那些本质上涉及基本权利与自由的敏感个人数据，因其处理背景可能对基本权利与自由构成重大风险，理应获得特殊保护。此类数据应包含揭示种族或民族起源的个人数据，但需特别说明：本指令中使用的‘种族起源’术语，并不意味着欧盟接受任何试图

to determine the existence of separate human races. Such personal data should not be processed, unless processing is subject to appropriate safeguards for the rights and freedoms of the data subject laid down by law and is allowed in cases authorised by law; where not already authorised by such a law, the processing is necessary to protect the vital interests of the data subject or of another person; or the processing relates to data which are manifestly made public by the data subject. Appropriate safeguards for the rights and freedoms of the data subject could include the possibility to collect those data only in connection with other data on the natural person concerned, the possibility to secure the data collected adequately, stricter rules on the access of staff of the competent authority to the data and the prohibition of transmission of those data. The processing of such data should also be allowed by law where the data subject has explicitly agreed to the processing that is particularly intrusive to him or her. However, the consent of the data subject should not provide in itself a legal ground for processing such sensitive personal data by competent authorities.

(38) The data subject should have the right not to be subject to a decision evaluating personal aspects relating to him or her which is based solely on automated processing and which produces adverse legal effects concerning, or significantly affects, him or her. In any case, such processing should be subject to suitable safeguards, including the provision of specific information to the data subject and the right to obtain human intervention, in particular to express his or her point of view, to obtain an explanation of the decision reached after such assessment or to challenge the decision. Profiling that results in discrimination against natural persons on the basis of personal data which are by their nature particularly sensitive in relation to fundamental rights and freedoms should be prohibited under the conditions laid down in Articles 21 and 52 of the Charter.

(39) In order to enable him or her to exercise his or her rights, any information to the data subject should be easily accessible, including on the website of the controller, and easy to understand, using clear and plain language. Such information should be adapted to the needs of vulnerable persons such as children.

(40) Modalities should be provided for facilitating the exercise of the data subject's rights under the provisions adopted pursuant to this Directive, including mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and restriction of processing. The controller should be obliged to respond to requests of the data subject without undue delay, unless the controller applies limitations to data subject rights in accordance with this Directive. Moreover, if requests are manifestly unfounded or excessive, such as where the data subject unreasonably and repetitiously requests information or where the data subject abuses his or her right to receive information, for example, by providing false or misleading information when making the request, the controller should be able to charge a reasonable fee or refuse to act on the request.

(41) Where the controller requests the provision of additional information necessary to confirm the identity of the data subject, that information should be processed only for that specific purpose and should not be stored for longer than needed for that purpose.

(42) At least the following information should be made available to the data subject: the identity of the controller, the existence of the processing operation, the purposes of the processing, the right to lodge a complaint and the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing. This could take place on the website of the competent authority. In addition, in specific cases and in order to enable the exercise of his or her rights, the data subject should be informed of the legal basis for the processing and of how long the data will be stored, in so far as such further information is necessary, taking into account the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.

(43) A natural person should have the right of access to data which has been collected concerning him or her, and to exercise this right easily and at reasonable intervals, in order to be aware of and verify the lawfulness of the processing. Every data subject should therefore have the right to know, and obtain communications about, the purposes for which the data are processed, the period during which the data are processed and the recipients of the data, including those in third countries. Where such communications include information as to the origin of the personal data, the information should not reveal the identity of natural persons, in particular confidential sources. For that right to be complied with, it is sufficient that the data subject be in possession of a full summary of those data in an intelligible form, that is to say a form which allows that data subject to become aware of those data and to verify that they are accurate and processed in accordance with this Directive, so that it

为判定是否存在不同人类种族。此类个人数据的处理应遵循以下原则：除非处理过程符合法律规定的数据主体权利与自由保障措施，且属于法律授权情形；若未获法律授权，处理行为必须保护数据主体或他人的重要权益；或处理涉及数据主体已明确公开的信息。保障数据主体权利与自由的适当措施可包括：仅在关联相关自然人的其他数据时收集该数据、确保数据收集充分可靠、对主管部门工作人员访问数据实施更严格管控、禁止数据传输。当数据主体明确同意处理对其具有特别侵入性的数据时，法律亦应允许此类数据处理。但需注意，数据主体的同意本身不应成为主管部门处理此类敏感个人数据的法定依据。

(38) 数据主体应当享有不被要求接受仅基于自动化处理且可能对其产生不利法律后果或重大影响的个人数据评估决定的权利。此类处理必须配备适当保障措施，包括向数据主体提供具体信息、保障其获得人工干预的权利——特别是表达观点的权利、获取评估后决策理由的权利以及提出异议的权利。根据《欧洲人权公约》第21条和第52条规定，若基于个人数据（这些数据本质上涉及基本权利和自由的敏感领域）进行的画像分析会导致对自然人的歧视，应当予以禁止。

(39) 为保障数据主体行使权利，所有相关信息（包括控制者网站内容）均应便于获取，并采用清晰简明的语言确保易懂性。此类信息需特别考虑儿童等弱势群体的实际需求。

(40) 应建立相应机制，保障数据主体根据本指令条款行使权利，包括建立免费获取（适用时）个人数据访问、更正或删除及限制处理的请求机制。数据控制者应无延迟地回应数据主体的请求，除非其依据本指令对数据主体权利施加限制。此外，若请求明显缺乏依据或过度，例如数据主体不合理重复索取信息，或滥用知情权（如在请求时提供虚假或误导性信息），数据控制者有权收取合理费用或拒绝处理该请求。

(41) 若控制者要求提供确认数据主体身份所需的补充信息，则该信息仅应为该特定目的处理，且存储时间不得超过该目的所需。

(42) 数据主体至少应获知以下信息：控制者的身份、数据处理操作的存在、处理目的、投诉权以及向控制者请求访问、更正或删除个人数据或限制处理的权利。这些信息可通过主管机构的网站获取。此外，在特定情况下，为确保数据主体能够行使权利，应告知其数据处理的法律依据及数据存储期限（如需补充说明），并结合数据处理的具体情形，以保障数据主体获得公平处理。

(43) 自然人应当享有查阅与其相关的个人数据的权利，并有权在合理的时间间隔内便捷行使该权利，以便了解并核实数据处理的合法性。因此，每位数据主体都应有权获知并获取关于数据处理目的、处理期限及接收方（包括第三国接收方）的说明。若说明内容涉及个人数据来源信息，相关说明不得泄露自然人的身份信息，特别是涉及保密来源的信息。为确保该权利得到切实保障，只需数据主体能以易于理解的形式获取完整数据摘要即可——即该摘要应使数据主体能够了解数据内容，并核实数据是否准确且符合本指令要求，从而确保其

is possible for him or her to exercise the rights conferred on him or her by this Directive. Such a summary could be provided in the form of a copy of the personal data undergoing processing.

(44) Member States should be able to adopt legislative measures delaying, restricting or omitting the information to data subjects or restricting, wholly or partly, the access to their personal data to the extent that and as long as such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned, to avoid obstructing official or legal inquiries, investigations or procedures, to avoid prejudicing the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, to protect public security or national security, or to protect the rights and freedoms of others. The controller should assess, by way of a concrete and individual examination of each case, whether the right of access should be partially or completely restricted.

(45) Any refusal or restriction of access should in principle be set out in writing to the data subject and include the factual or legal reasons on which the decision is based.

(46) Any restriction of the rights of the data subject must comply with the Charter and with the ECHR, as interpreted in the case-law of the Court of Justice and by the European Court of Human Rights respectively, and in particular respect the essence of those rights and freedoms.

(47) A natural person should have the right to have inaccurate personal data concerning him or her rectified, in particular where it relates to facts, and the right to erasure where the processing of such data infringes this Directive. However, the right to rectification should not affect, for example, the content of a witness testimony. A natural person should also have the right to restriction of processing where he or she contests the accuracy of personal data and its accuracy or inaccuracy cannot be ascertained or where the personal data have to be maintained for purpose of evidence. In particular, instead of erasing personal data, processing should be restricted if in a specific case there are reasonable grounds to believe that erasure could affect the legitimate interests of the data subject. In such a case, restricted data should be processed only for the purpose which prevented their erasure. Methods to restrict the processing of personal data could include, inter alia, moving the selected data to another processing system, for example for archiving purposes, or making the selected data unavailable. In automated filing systems the restriction of processing should in principle be ensured by technical means. The fact that the processing of personal data is restricted should be indicated in the system in such a manner that it is clear that the processing of the personal data is restricted. Such rectification or erasure of personal data or restriction of processing should be communicated to recipients to whom the data have been disclosed and to the competent authorities from which the inaccurate data originated. The controllers should also abstain from further dissemination of such data.

(48) Where the controller denies a data subject his or her right to information, access to or rectification or erasure of personal data or restriction of processing, the data subject should have the right to request that the national supervisory authority verify the lawfulness of the processing. The data subject should be informed of that right. Where the supervisory authority acts on behalf of the data subject, the data subject should be informed by the supervisory authority at least that all necessary verifications or reviews by the supervisory authority have taken place. The supervisory authority should also inform the data subject of the right to seek a judicial remedy.

(49) Where the personal data are processed in the course of a criminal investigation and court proceedings in criminal matters, Member States should be able to provide that the exercise the right to information, access to and rectification or erasure of personal data and restriction of processing is carried out in accordance with national rules on judicial proceedings.

(50) 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 should be able to demonstrate that processing activities are in compliance with this Directive. Such 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. The measures taken by the controller should include drawing up and implementing specific safeguards in respect of the treatment of personal data of vulnerable natural persons, such as children.

(51) The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from 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 data protected by professional secrecy, unauthorised reversal of pseudonymisation or any other

他或她有权行使本指令赋予的权利。此类摘要可采用正在处理的个人数据副本的形式提供。

(44) 成员国应有权采取立法措施，对数据主体的信息披露进行延迟、限制或豁免，或对其个人数据的访问权限实施全部或部分限制。但需满足以下条件：该措施须在充分尊重相关自然人基本权利和合法权益的前提下，构成民主社会中必要且相称的措施；不得妨碍官方或法律调查、侦查或程序的开展；不得妨碍刑事犯罪的预防、侦查、侦破或起诉，或刑事处罚的执行；不得损害公共安全或国家安全；亦不得侵犯他人权利与自由。数据控制者应通过具体个案审查，评估是否应对访问权实施部分或全部限制。

(45) 任何拒绝或限制访问的行为原则上均应以书面形式告知数据主体，并说明该决定所依据的事实或法律依据。

(46) 任何对数据主体权利的限制，均须符合《欧洲人权公约》及其《宪章》的规定，且须符合欧洲人权法院与欧洲人权法院判例法的解释，尤其须尊重这些权利与自由的本质。

(47) 自然人应当有权要求更正与其相关的不准确个人数据，特别是涉及事实性信息时，当数据处理行为违反本指令规定时，更应享有删除权。但需注意，更正权不应影响证人证言的内容等关键信息。当个人对数据准确性存疑、无法确认数据真伪，或为证据保存需要保留数据时，自然人同样享有限制处理的权利。特别需要强调的是，若存在合理依据认为删除可能损害数据主体的合法权益，则应采取限制处理而非直接删除。在此情形下，受限处理仅限于防止删除的原始目的。限制个人数据处理的具体措施包括：将选定数据迁移至其他处理系统（如归档存储），或采取数据不可用等技术手段。在自动化归档系统中，原则上应通过技术手段确保数据处理的限制。系统中应以清晰可见的方式明确标注个人数据处理的限制。此类数据更正、删除或处理限制措施，必须向数据接收方及数据来源的主管部门进行通报。数据控制者还应停止进一步传播此类数据。

(48) 当控制者剥夺数据主体获取信息权、访问权、更正或删除个人数据权或限制处理权时，数据主体应有权要求国家监管机构核查处理行为的合法性。监管机构应当告知数据主体此项权利。若监管机构代表数据主体行事，应至少告知其已完成所有必要的核查或审查程序。监管机构还应告知数据主体寻求司法救济的权利。

(49) 当个人数据在刑事调查及刑事诉讼程序中被处理时，成员国应确保信息权、数据访问权、更正或删除权以及数据处理限制权的行使，均符合本国司法程序的相关规定。

(50) 数据控制者应对自身或代表其进行的任何个人数据处理行为承担相应责任。具体而言，数据控制者必须采取适当且有效的措施，并能证明其处理活动符合本指令要求。这些措施需综合考量数据处理的性质、范围、背景及目的，同时评估对自然人权利与自由可能造成的风险。数据控制者应制定并落实针对弱势群体（如儿童）个人数据处理的专项保护措施。

(51) 数据处理可能对自然人的权利和自由造成不同程度的风险，这些风险可能引发人身伤害、财产损失或非物质损害，具体包括：可能导致歧视、身份盗用或欺诈行为；造成经济损失；损害个人声誉；泄露受职业保密保护的数据；未经授权撤销匿名化处理；以及其他任何后果。

significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs or trade union membership; where genetic data or biometric data are processed in order to uniquely identify a person or where data concerning health or data concerning sex life and sexual orientation or criminal convictions and offences or related security measures are processed; where personal aspects are evaluated, in particular analysing and 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 children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.

(52) The likelihood and severity of the risk 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, through which it is established whether data-processing operations involve a high risk. A high risk is a particular risk of prejudice to the rights and freedoms of data subjects.

(53) The protection of the rights and freedoms of natural persons with regard to the processing of personal data requires that appropriate technical and organisational measures are taken, to ensure that the requirements of this Directive are met. The implementation of such measures should not depend solely on economic considerations. In order to be able to demonstrate compliance with this Directive, the controller should adopt internal policies and implement measures which adhere in particular to the principles of data protection by design and data protection by default. Where the controller has carried out a data protection impact assessment pursuant to this Directive, the results should be taken into account when developing those measures and procedures. The measures could consist, inter alia, of the use of pseudonymisation, as early as possible. The use of pseudonymisation for the purposes of this Directive can serve as a tool that could facilitate, in particular, the free flow of personal data within the area of freedom, security and justice.

(54) 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 attribution of the responsibilities set out in this Directive, 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.

(55) The carrying-out of processing by a processor should be governed by a legal act including a contract binding the processor to the controller and stipulating, in particular, that the processor should act only on instructions from the controller. The processor should take into account the principle of data protection by design and by default.

(56) In order to demonstrate compliance with this Directive, the controller or processor should maintain records regarding all categories of processing activities under its responsibility. Each controller and processor should be obliged to cooperate with the supervisory authority and make those records available to it on request, so that they might serve for monitoring those processing operations. The controller or the processor processing personal data in non-automated processing systems should have in place effective methods of demonstrating the lawfulness of the processing, of enabling self-monitoring and of ensuring data integrity and data security, such as logs or other forms of records.

(57) Logs should be kept at least for operations in automated processing systems such as collection, alteration, consultation, disclosure including transfers, combination or erasure. The identification of the person who consulted or disclosed personal data should be logged and from that identification it should be possible to establish the justification for the processing operations. The logs should solely be used for the verification of the lawfulness of the processing, self-monitoring, for ensuring data integrity and data security and criminal proceedings. Self-monitoring also includes internal disciplinary proceedings of competent authorities.

(58) A data protection impact assessment should be carried out by the controller where the processing operations are likely to result in a high risk to the rights and freedoms of data subjects by virtue of their nature, scope or purposes, which should include, in particular, the measures, safeguards and mechanisms envisaged to ensure the protection of personal data and to demonstrate compliance with this Directive. Impact assessments should cover relevant systems and processes of processing operations, but not individual cases.

重大经济或社会劣势；数据主体可能被剥夺权利与自由，或无法行使对个人数据的控制权；处理的个人数据涉及种族或民族起源、政治观点、宗教或哲学信仰、工会会员身份；处理遗传数据或生物识别数据以唯一识别个人，或处理涉及健康状况、性生活与性取向、犯罪记录及相关安全措施的数据；评估个人特征，特别是分析和预测工作表现、经济状况、健康状况、个人偏好或兴趣、可靠性或行为、位置或移动情况，以创建或使用个人档案；处理弱势自然人（尤其是儿童）的个人数据；或处理涉及大量个人数据且影响众多数据主体的情况。

(52) 应根据数据处理的性质、范围、背景及目的来确定风险的可能性和严重程度。风险评估应基于客观判断，以确定数据处理操作是否涉及高风险。高风险特指可能损害数据主体权利与自由的特定风险。

(53) 为保障自然人在个人数据处理中的权利与自由，必须采取适当的技术和组织措施，确保符合本指令要求。实施这些措施不应仅基于经济考量。为证明符合本指令要求，数据控制者应制定内部政策并采取措施，尤其要遵循“数据保护设计原则”和“默认数据保护原则”。若数据控制者已根据本指令完成数据保护影响评估，则在制定相关措施和程序时应参考评估结果。这些措施可包括尽早采用假名化处理等手段。根据本指令，假名化处理可作为促进个人数据在自由、安全与正义领域自由流动的有效工具。

(54) 为保障数据主体的权利与自由，同时明确控制者和处理者的责任与义务（包括监管机构的监督措施），本指令明确规定了相关责任归属。具体而言，当控制者与其他控制者共同确定数据处理的目的和方式，或处理操作由第三方代表控制者执行时，均需明确责任归属。

(55) 数据处理者在执行数据处理时，应受法律行为约束，包括与控制者签订的合同，该合同须明确规定：处理者仅能依据控制者的指令行事。同时，处理者在设计和默认情况下均须遵循数据保护原则。

(56) 为证明符合本指令要求，数据控制者或处理者应保存其负责的所有类型数据处理活动的记录。各数据控制者和处理者必须配合监管机构工作，应监管机构要求提供相关记录，以便用于监督数据处理活动。对于使用非自动化处理系统处理个人数据的数据控制者或处理者，应建立有效机制以证明数据处理的合法性、实现自我监督，并确保数据完整性和安全性，例如通过日志或其他形式的记录。

(57) 在自动化处理系统中，包括收集、修改、查阅、披露（含转移、合并或删除）等操作时，应至少保留日志记录。需记录查阅或披露个人数据的人员身份信息，并通过该身份信息追溯相关处理操作的正当理由。日志记录仅用于验证处理行为的合法性、开展自我监督、保障数据完整性与安全，以及支持刑事诉讼程序。自我监督机制还涵盖主管部门的内部纪律审查程序。

(58) 当数据处理操作因其性质、范围或目的可能对数据主体的权利和自由构成高风险时，控制者应当进行数据保护影响评估。该评估应特别包括为确保个人数据保护所设想的措施、保障措施及机制，并证明符合本指令要求。影响评估应涵盖相关数据处理系统的运作流程，但不涉及具体个案。

(59) In order to ensure effective protection of the rights and freedoms of data subjects, the controller or processor should consult the supervisory authority, in certain cases, prior to the processing.

(60) In order to maintain security and to prevent processing that infringes this Directive, the controller or processor should evaluate the risks inherent in the processing and should implement measures to mitigate those risks, such as encryption. Such measures should ensure an appropriate level of security, including confidentiality and take into account the state of the art, the costs of implementation in relation to the risk and the nature of the personal data to be protected. In assessing data security risks, consideration should be given to the risks that are presented by data processing, such as the accidental or unlawful destruction, loss, alteration or 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. The controller and processor should ensure that the processing of personal data is not carried out by unauthorised persons.

(61) 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 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.

(62) Natural persons should be informed without undue delay where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, in order to allow them to take the necessary precautions. The communication should describe the nature of the personal data breach and include recommendations for the natural person concerned to mitigate potential adverse effects. Communication to data subjects should be made as soon as reasonably feasible, in close cooperation with the supervisory authority, and respecting guidance provided by it or other relevant authorities. For example, the need to mitigate an immediate risk of damage would call for a prompt communication to data subjects, whereas the need to implement appropriate measures against continuing or similar data breaches may justify more time for the communication. Where avoiding obstruction of official or legal inquiries, investigations or procedures, avoiding prejudice to the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties, protecting public security, protecting national security or protecting the rights and freedoms of others cannot be achieved by delaying or restricting the communication of a personal data breach to the natural person concerned, such communication could, in exceptional circumstances, be omitted.

(63) The controller should designate a person who would assist it in monitoring internal compliance with the provisions adopted pursuant to this Directive, except where a Member State decides to exempt courts and other independent judicial authorities when acting in their judicial capacity. That person could be a member of the existing staff of the controller who received special training in data protection law and practice in order to acquire expert knowledge in that field. The necessary level of expert knowledge should be determined, in particular, according to the data processing carried out and the protection required for the personal data processed by the controller. His or her task could be carried out on a part-time or full-time basis. A data protection officer may be appointed jointly by several controllers, taking into account their organisational structure and size, for example in the case of shared resources in central units. That person can also be appointed to different positions within the structure of the relevant controllers. That person should help the controller and the employees processing personal data by informing and advising them on compliance with their relevant data protection obligations. Such data protection officers should be in a position to perform their duties and tasks in an independent manner in accordance with Member State law.

(64) Member States should ensure that a transfer to a third country or to an international organisation takes place only if necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, and that

(59) 为有效保障数据主体的权利与自由，数据控制者或处理者在特定情况下应于处理前咨询监管机构。

(60) 为保障安全并防止违反本指令的处理行为，控制者或处理者应评估数据处理固有风险，并采取加密等措施降低风险。相关措施需确保适当的安全水平，包括保密性，同时需考量技术现状、实施成本与风险之间的平衡，以及待保护个人数据的性质。在评估数据安全风险时，应重点考虑数据处理可能引发的风险，例如传输、存储或处理过程中个人数据的意外或非法损毁、丢失、篡改或未经授权的泄露或访问，这些行为可能导致人身、财产或非物质损害。控制者和处理者必须确保个人数据处理不被未经授权的人员实施。

(61) 若未能及时妥善处理个人数据泄露事件，可能对自然人造成人身、财产或精神损害，包括但不限于：个人数据控制权丧失、权利受限、遭受歧视、身份盗用或欺诈、经济损失、匿名化处理遭非法撤销、声誉受损、受职业保密保护的个人数据机密性丧失，以及其他重大经济或社会不利影响。因此，数据控制者一旦发现个人数据泄露事件，应立即向监管机构通报，且在可行情况下，最迟应在发现后72小时内完成通知，除非根据问责原则能够证明该泄露事件不会对自然人的权利和自由构成风险。若无法在72小时内完成通知，应说明延迟原因，并可分阶段提供信息而不造成进一步延误。

(62) 当个人数据泄露可能对自然人的权利和自由构成重大风险时，应立即通知相关个人，以便其采取必要防范措施。通知内容需详细说明数据泄露的具体情况，并提供具体建议帮助当事人减轻潜在负面影响。通知数据主体应当与监管机构密切配合，在合理可行的最短时间内完成，同时遵循监管机构或其他相关机构的指导原则。例如，若需立即消除损害风险，应尽快通知数据主体；而若需针对持续或类似数据泄露事件采取应对措施，则可适当延长通知时间。若因延迟或限制向相关自然人通报个人数据泄露事件，将无法避免妨碍公务或合法调查程序、妨碍犯罪行为的预防、侦查、起诉或刑事处罚的执行、妨碍公共安全、妨碍国家安全或妨碍他人权利与自由的保护，则在特殊情况下可予以豁免。

(63) 数据控制者应当指定一名专职人员协助监督其内部对本指令所采纳条款的遵守情况，但成员国决定豁免法院及其他独立司法机关在司法职能行使时适用本指令的除外。该人员可为数据控制者现有员工中接受过数据保护法律与实务专项培训的成员，以获取该领域的专业知识。所需的专业知识水平应根据数据处理类型及所处理个人数据的保护要求来确定。该人员可采用兼职或全职工作模式。在考虑组织架构和规模因素（例如中央部门共享资源的情况下），多个数据控制者可联合任命数据保护官。该人员亦可在相关数据控制者内部结构中担任不同职务。该人员应协助数据控制者及处理个人数据的员工，通过告知并指导其履行相关数据保护义务。此类数据保护官应能依据成员国法律独立履行其职责。

(64) 成员国应确保，只有在预防、调查、侦查或起诉刑事犯罪或执行刑事处罚（包括防范和防止对公共安全的威胁）确有必要时，才可将案件移交第三国或国际组织，并且

the controller in the third country or international organisation is an authority competent within the meaning of this Directive. A transfer should be carried out only by competent authorities acting as controllers, except where processors are explicitly instructed to transfer on behalf of controllers. Such a transfer may take place in cases where the Commission has decided that the third country or international organisation in question ensures an adequate level of protection, where appropriate safeguards have been provided, or where derogations for specific situations apply. Where personal data are transferred from the Union to controllers, to processors or to other recipients in third countries or international organisations, the level of protection of natural persons provided for in the Union by this Directive should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers or processors in the same or in another third country or international organisation.

(65) Where personal data are transferred from a Member State to third countries or international organisations, such a transfer should, in principle, take place only after the Member State from which the data were obtained has given its authorisation to the transfer. The interests of efficient law-enforcement cooperation require that where the nature of a threat to the public security of a Member State or a third country or to the essential interests of a Member State is so immediate as to render it impossible to obtain prior authorisation in good time, the competent authority should be able to transfer the relevant personal data to the third country or international organisation concerned without such a prior authorisation. Member States should provide that any specific conditions concerning the transfer should be communicated to third countries or international organisations. Onward transfers of personal data should be subject to prior authorisation by the competent authority that carried out the original transfer. When deciding on a request for the authorisation of an onward transfer, the competent authority that carried out the original transfer should take due account of all relevant factors, including the seriousness of the criminal offence, the specific conditions subject to which, and the purpose for which, the data was originally transferred, the nature and conditions of the execution of the criminal penalty, and the level of personal data protection in the third country or an international organisation to which personal data are onward transferred. The competent authority that carried out the original transfer should also be able to subject the onward transfer to specific conditions. Such specific conditions can be described, for example, in handling codes.

(66) The Commission should be able to decide with effect for the entire Union that certain third countries, a territory or one or more specified sectors within a third country, or an international organisation, offer an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third countries or international organisations which are considered to provide such a level of protection. In such cases, transfers of personal data to those countries should be able to take place without the need to obtain any specific authorisation, except where another Member State from which the data were obtained has to give its authorisation to the transfer.

(67) 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 protection essentially equivalent to that ensured within the Union, in particular where data are processed in one or several specific sectors. In particular, the third country should ensure effective independent data protection supervision and 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.

(68) Apart from the international commitments the third country or international organisation has entered into, the Commission should also 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 with

第三国或国际组织的控制者是指本指令所定义的具有管辖权的主管机构。数据传输仅应由作为控制者的主管机构执行，除非数据处理者被明确授权代表控制者进行传输。此类传输可在以下情形下实施：欧盟委员会认定相关第三国或国际组织能提供充分的保护水平、已采取适当保障措施，或适用特定情况的豁免条款。当个人数据从欧盟传输至第三国或国际组织的控制者、数据处理者或其他接收方时，本指令在欧盟层面为自然人提供的保护水平不得被削弱，包括当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或数据处理者时。

(65) 当个人数据从成员国转移至第三国或国际组织时，原则上应仅在数据来源国授权后方可进行。为保障高效执法合作，若某项威胁对成员国或第三国的公共安全，或对成员国核心利益构成的紧迫性，致使无法及时取得事先授权，主管机关应有权在无需事先授权的情况下，将相关个人数据转移至相关第三国或国际组织。成员国应规定，所有涉及数据转移的具体条件均须向第三国或国际组织明确告知。后续个人数据的转移，须经执行原转移的主管机关事先批准。在审批数据转接授权申请时，原数据转移主管部门应当综合考量以下关键因素：犯罪行为的严重程度、数据转移的具体适用条件及原始目的、刑事处罚执行的性质与条件，以及接收方国家或国际组织的个人数据保护水平。该主管部门还应有权为数据转接设定具体条件，例如通过制定操作规范等方式予以明确。

(66) 欧盟委员会应当有权就整个联盟范围内作出决定，认定某些第三国、某领土或第三国境内一个或多个特定领域，或某个国际组织，已达到充分的数据保护标准。此举将为联盟内认定具备此类保护水平的第三国或国际组织提供法律确定性与统一性。在此情形下，向这些国家传输个人数据无需特别授权，但若数据来源国是其他成员国，则需获得该国的授权方可进行传输。

(67) 根据欧盟建立时所秉持的核心价值观，尤其是对人权的保护，欧盟委员会在评估第三国、第三国境内特定领土或特定领域时，应当综合考量该国对法治的遵守程度、司法公正的可及性，以及国际人权准则与标准的落实情况，同时评估其普通法与部门法体系，包括涉及公共安全、国防与国家安全、公共秩序及刑法的立法。针对第三国境内特定领土或特定领域的适格性评估决定，必须基于明确客观的标准，例如该国特定数据处理活动的性质，以及现行法律标准与法规的适用范围。第三国应当提供充分保障，确保其数据保护水平基本等同于欧盟境内标准，特别是在数据处理涉及一个或多个特定领域的情况下。具体而言，第三国应建立独立有效的数据保护监督机制，并与成员国数据保护主管部门建立合作机制；同时，应保障数据主体享有切实可行的可执行权利，以及有效的行政与司法救济途径。

(68) 除第三国或国际组织已作出的国际承诺外，欧盟委员会还应考虑其参与多边或区域体系所产生的义务，特别是涉及个人数据保护的义务及其履行情况。需特别注意第三国加入《欧洲委员会1981年1月28日关于个人数据自动处理的保护公约》及其附加议定书的情况。欧盟委员会应与相关方进行磋商。

the European Data Protection Board established by Regulation (EU) 2016/679 (the 'Board') when assessing the level of protection in third countries or international organisations. The Commission should also take into account any relevant Commission adequacy decision adopted in accordance with Article 45 of Regulation (EU) 2016/679.

(69) The Commission should monitor the functioning of decisions on the level of protection in a third country, a territory or a specified sector within a third country, or an international organisation. In its adequacy decisions, the Commission should provide for a periodic review mechanism of their functioning. That periodic review should be undertaken in consultation with the third country or international organisation in question and should take into account all relevant developments in the third country or international organisation.

(70) The Commission should also be able to 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 Directive relating to transfers subject to appropriate safeguards and derogations for specific situations are fulfilled. Provision should be made for procedures 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.

(71) Transfers not based on such an adequacy decision should be allowed only where appropriate safeguards have been provided in a legally binding instrument which ensures the protection of personal data or where the controller has assessed all the circumstances surrounding the data transfer and, on the basis of that assessment, considers that appropriate safeguards with regard to the protection of personal data exist. Such legally binding instruments could, for example, be legally binding bilateral agreements which have been concluded by the Member States and implemented in their legal order and which could be enforced by their data subjects, ensuring compliance with data protection requirements and the rights of the data subjects, including the right to obtain effective administrative or judicial redress. The controller should be able to take into account cooperation agreements concluded between Europol or Eurojust and third countries which allow for the exchange of personal data when carrying out the assessment of all the circumstances surrounding the data transfer. The controller should be able to also take into account the fact that the transfer of personal data will be subject to confidentiality obligations and the principle of specificity, ensuring that the data will not be processed for other purposes than for the purposes of the transfer. In addition, the controller should take into account that the personal data will not be used to request, hand down or execute a death penalty or any form of cruel and inhuman treatment. While those conditions could be considered to be appropriate safeguards allowing the transfer of data, the controller should be able to require additional safeguards.

(72) Where no adequacy decision or appropriate safeguards exist, a transfer or a category of transfers could take place only in specific situations, if necessary to protect the vital interests of the data subject or another person, or to safeguard legitimate interests of the data subject where the law of the Member State transferring the personal data so provides; for the prevention of an immediate and serious threat to the public security of a Member State or a third country; in an individual case 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; or in an individual case for the establishment, exercise or defence of legal claims. Those derogations should be interpreted restrictively and should not allow frequent, massive and structural transfers of personal data, or large-scale transfers of data, but should be limited to data strictly necessary. Such transfers should be documented and should be made available to the supervisory authority on request in order to monitor the lawfulness of the transfer.

(73) Competent authorities of Member States apply bilateral or multilateral international agreements in force, concluded with third countries in the field of judicial cooperation in criminal matters and police cooperation, for the exchange of relevant information to allow them to perform their legally assigned tasks. In principle, this takes place through, or at least with, the cooperation of the authorities competent in the third countries concerned for the purposes of this Directive, sometimes even in the absence of a bilateral or multilateral international agreement. However, in specific individual cases, the regular procedures requiring contacting such an authority in the third country may be ineffective or inappropriate, in particular because the transfer could not be carried out in a timely manner, or because that authority in the third country does not respect the rule of law or international human rights norms and standards, so that competent authorities of Member States could decide to transfer personal data directly to recipients established in those third countries. This may be the case where there is an urgent need to transfer personal data to save the life of a person who is in danger of becoming a victim of a criminal offence or in the interest of preventing an imminent perpetration of a crime, including terrorism. Even if

根据欧盟第2016/679号条例设立的欧洲数据保护委员会（以下简称‘委员会’）在评估第三国或国际组织的数据保护水平时，欧盟委员会还应考虑根据该条例第45条通过的任何相关充分性决定。

(69) 欧盟委员会应当监督关于第三国、第三国领土或特定部门内保护水平的决定的执行情况，以及国际组织的相关决定。在评估这些决定是否充分时，委员会应建立定期审查机制。此类定期审查需与相关第三国或国际组织协商进行，并充分考虑该国或该组织的所有相关发展动态。

(70) 欧盟委员会还应认识到，若第三国、其领土或特定部门，或国际组织已无法提供充分的数据保护水平，则应禁止向该国或该组织传输个人数据，除非满足本指令中关于需采取适当保障措施及特定情形例外条款的传输要求。委员会应建立与相关第三国或国际组织的磋商机制。委员会应及时向相关方说明原因，并通过磋商解决数据保护不足的问题。

(71) 对于未基于充分性决定的数据传输，只有在以下两种情形下方可允许：一是相关法律文件已提供充分保障个人数据安全的适当措施；二是数据控制者在全面评估数据传输相关情况后，确认已采取适当保护措施。这类具有法律约束力的文件可以是成员国签订并实施的双边协议，数据主体可依据这些协议要求相关方遵守数据保护规定，保障其权利（包括获得有效行政或司法救济的权利）。在评估数据传输相关情况时，数据控制者还应考虑欧洲刑警组织或欧洲司法组织与第三国签订的合作协议，这些协议允许进行个人数据交换。数据控制者还应充分考虑，个人数据的转移必须遵守保密义务和特定性原则，确保数据处理目的仅限于转移时所指定的用途。此外，控制者还需注意，个人数据不得用于请求、下达或执行死刑，或实施任何形式的残酷非人道待遇。虽然这些条件可视为允许数据转移的适当保障措施，但控制者仍有权要求采取额外的保护措施。

(72) 在缺乏充分性决定或适当保障措施的情况下，只有在特定情形下方可进行数据转移或特定类型的数据转移，具体包括：为保护数据主体或他人的重要利益；根据个人数据转移成员国的法律规定，为保障数据主体的合法权益；为防范对成员国或第三国公共安全构成直接且严重威胁；在个案中为预防、调查、侦查或起诉刑事犯罪或执行刑事处罚（包括防范和预防公共安全威胁）；或为确立、行使或辩护法律主张。此类例外情形应严格解释，不得允许频繁、大规模或结构性的数据转移，也不得允许大规模数据转移，而应仅限于严格必要的数据。此类转移应有书面记录，并应根据监管机构要求提供，以便监督转移行为的合法性。

(73) 成员国主管机关在刑事司法合作和警务合作领域，会依据与第三国签订的现行双边或多边国际协议，通过信息交换协助完成法定职责。原则上，这种信息共享需通过或至少在相关第三国主管机关的配合下进行，有时甚至无需双边或多边协议。但在个别特殊情况下，常规程序可能因存在以下问题而失效或不适用：数据传输未能及时完成，或第三国主管机关不遵守法治原则及国际人权规范标准。此时成员国主管机关可直接将个人数据传输至第三国境内设立的接收机构。当存在紧急情况时，可能需要转移个人数据以挽救生命，例如当某人面临成为刑事犯罪受害者的危险，或为防止即将发生的犯罪（包括恐怖主义）而采取行动。即使

such a transfer between competent authorities and recipients established in third countries should take place only in specific individual cases, this Directive should provide for conditions to regulate such cases. Those provisions should not be considered to be derogations from any existing bilateral or multilateral international agreements in the field of judicial cooperation in criminal matters and police cooperation. Those rules should apply in addition to the other rules of this Directive, in particular those on the lawfulness of processing and Chapter V.

(74) Where personal data move across borders it may put at increased risk the ability of natural persons to exercise data protection rights to protect themselves from the unlawful use or disclosure of those data. 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 and inconsistent legal regimes. Therefore, there is a need to promote closer cooperation among data protection supervisory authorities to help them exchange information with their foreign counterparts.

(75) The establishment in Member States of supervisory authorities that are able to exercise their functions with complete independence is an essential component of the protection of natural persons with regard to the processing of their personal data. The supervisory authorities should monitor the application of the provisions adopted pursuant to this Directive and should contribute to their consistent application throughout the Union in order to protect natural persons with regard to the processing of their personal data. To that end, the supervisory authorities should cooperate with each other and with the Commission.

(76) Member States may entrust a supervisory authority already established under Regulation (EU) 2016/679 with the responsibility for the tasks to be performed by the national supervisory authorities to be established under this Directive.

(77) Member States should be allowed to establish more than one supervisory authority to reflect their constitutional, organisational and administrative structure. Each supervisory authority should be provided with the financial and human resources, premises and infrastructure, which are necessary for the effective performance of their tasks, including for the tasks 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.

(78) Supervisory authorities should be subject to independent control or monitoring mechanisms regarding their financial expenditure, provided that such financial control does not affect their independence.

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

(80) While this Directive applies also to the activities of national courts and other judicial authorities, the competence of the supervisory authorities should not cover the processing of personal data where courts are acting in their judicial capacity, in order to safeguard the independence of judges in the performance of their judicial tasks. That exemption should be limited to judicial activities in court cases and not apply to other activities where judges might be involved in accordance with Member State law. Member States should also be able to provide that the competence of the supervisory authority does not cover the processing of personal data of other independent judicial authorities when acting in their judicial capacity, for example public prosecutor's office. In any event, the compliance with the rules of this Directive by the courts and other independent judicial authorities is always subject to independent supervision in accordance with Article 8(3) of the Charter.

在第三国设立的主管机关与接收方之间进行此类移交时，仅应在特定个案中实施。本指令应为此类案件规定相应的监管条件。相关条款不得被视为对刑事司法合作及警务合作领域现有双边或多边国际协议的任何背离。这些规则除本指令其他条款外，还应适用，特别是关于数据处理合法性的规定以及第五章的相关条款。

(74) 当个人数据跨境流动时，自然人行使数据保护权利以防范数据被非法使用或泄露的能力可能面临更大风险。与此同时，监管机构可能发现难以追查境外活动或开展相关调查。跨境合作的努力也可能因预防或补救措施不足、法律制度不统一而受阻。因此，有必要推动数据保护监管机构加强协作，促进其与外国同行的信息互通。

(75) 在成员国设立能够完全独立行使职能的监管机构，是保护自然人在个人数据处理方面权益的重要组成部分。这些监管机构应当监督本指令所规定条款的实施，并为确保欧盟范围内各项规定的统一执行作出贡献，从而切实保障自然人在个人数据处理中的合法权益。为此，各监管机构之间以及与欧盟委员会之间应当开展密切合作。

(76) 成员国可委托根据欧盟第2016/679号条例已设立的监管机构，负责执行本指令所要求的国家监管机构应履行的职责。

(77) 成员国应被允许设立多个监管机构，以体现其宪法、组织架构和行政结构。每个监管机构都应获得必要的财政资源、人力资源、办公场所及基础设施，以确保其有效履行职责，包括与欧盟其他监管机构开展互助合作的相关任务。各监管机构应拥有独立的年度公共预算，该预算可纳入国家或联邦总预算体系。

(78) 监管机构的财务支出应受独立控制或监督机制约束，但此类财务管控不得影响其独立性。

(79) 成员国法律应明确规定监督机构成员的基本任职条件，尤其要规定：成员的任命应由议会、政府或成员国国家元首根据政府或政府成员、议会或其下议院的提议进行；或由成员国法律授权的独立机构通过透明程序任命。为确保监督机构的独立性，成员须秉持诚信履职，不得从事任何违背职责的行为，且在任期内不得从事任何不相容的职业（无论是否营利）。为保障监督机构的独立性，其工作人员应由监督机构自行遴选，必要时可引入成员国法律授权的独立机构参与选拔。

(80) 尽管本指令同样适用于各国法院及其他司法机构的活动，但为保障法官在履行司法职责时的独立性，监管机构的职权范围不应涵盖法院以司法身份行事时的个人数据处理行为。该豁免应仅限于法院审理案件时的司法活动，不适用于法官根据成员国法律可能参与的其他活动。成员国还可规定，当其他独立司法机构（如检察院）以司法身份行事时，监管机构的职权范围不包括其个人数据处理行为。无论如何，法院及其他独立司法机构遵守本指令规则的行为，始终须根据《宪章》第8条第3款接受独立监督。

(81) Each supervisory authority should handle complaints lodged by any data subject and should investigate the matter or transmit it to the competent supervisory authority. 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 provided to the data subject.

(82) In order to ensure effective, reliable and consistent monitoring of compliance with and enforcement of this Directive throughout the Union pursuant to the TFEU as interpreted by the Court of Justice, the supervisory authorities should have in each Member State the same tasks and effective powers, including investigative, corrective, and advisory powers which constitute necessary means to perform their tasks. However, their powers should not interfere with specific rules for criminal proceedings, including investigation and prosecution of criminal offences, or the independence of the judiciary. Without prejudice to the powers of prosecutorial authorities under Member State law, supervisory authorities should also have the power to bring infringements of this Directive to the attention of the judicial authorities or to engage in legal proceedings. The powers of supervisory authorities should be exercised in accordance with appropriate procedural safeguards laid down by 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 Directive, taking into account the circumstances of each individual case, respect the right of every person to be heard before any individual measure that would adversely affect the person concerned is taken, and avoiding superfluous costs and excessive inconvenience to the person concerned. Investigative powers as regards access to premises should be exercised in accordance with specific requirements in Member State law, such as the requirement to obtain a prior judicial authorisation. The adoption of a legally binding decision should be subject to judicial review in the Member State of the supervisory authority that adopted the decision.

(83) The supervisory authorities should assist one another in performing their tasks and provide mutual assistance, so as to ensure the consistent application and enforcement of the provisions adopted pursuant to this Directive.

(84) The Board should contribute to the consistent application of this Directive throughout the Union, including advising the Commission and promoting the cooperation of the supervisory authorities throughout the Union.

(85) Every data subject should have the right to lodge a complaint with a single supervisory authority and to an effective judicial remedy in accordance with Article 47 of the Charter where the data subject considers that his or her rights under provisions adopted pursuant to this Directive 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 competent 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 provided 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.

(86) Each natural or legal person should have the right to 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, that right does not encompass other measures of 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 Member State law. Those courts should exercise full jurisdiction which should include jurisdiction to examine all questions of fact and law relevant to the dispute before it.

(87) Where a data subject considers that his or her rights under this Directive are infringed, he or she should have the right to mandate a body which aims to protect the rights and interests of data subjects in relation to the

(81) 各监管机构应当受理数据主体提出的投诉，并对投诉事项进行调查或转交主管监管机构处理。投诉调查应根据具体案件情况，在司法审查框架内开展。监管机构应在合理期限内向数据主体通报投诉进展及处理结果。若案件需要进一步调查或需与其他监管机构协调，应当向数据主体提供阶段性信息。

(82) 为了确保根据欧盟法院解释的《通用数据保护条例》（TFEU）在整个联盟范围内有效、可靠且一致地监督和执行本指令，各成员国的监管机构应拥有相同的任务和有效的权力，包括调查、纠正和咨询权力，这些是履行其职责的必要手段。然而，这些权力不应干扰刑事诉讼的具体规则，包括对刑事犯罪的调查和起诉，也不应影响司法独立。在不影响成员国法律规定的检察机关权力的前提下，监管机构还应有权将本指令的违规行为提请司法机关注意或参与法律程序。监管机构的权力应按照欧盟和成员国法律规定的适当程序保障，公正、公平且在合理时间内行使。具体而言，各项措施在确保符合本指令要求时，应充分考虑个案具体情况，做到适当、必要且适度。在采取任何可能对当事人造成不利影响的措施前，必须尊重当事人的陈述权，避免产生不必要的开支和过度的不便。关于进入场所的调查权限，应依照成员国法律的具体规定行使，例如需事先取得司法授权的要求。具有法律约束力的决定的通过，应接受作出该决定的监督机构所在成员国的司法审查。

(83) 监管机构应相互协作履行职责，提供协助，以确保本指令所采纳条款的统一适用与执行。

(84) 理事会应推动该指令在欧盟范围内的统一实施，包括向欧盟委员会提供咨询意见，并促进欧盟各成员国监管机构之间的协作。

(85) 根据《欧盟通用数据保护条例》第47条规定，每位数据主体均有权向单一监管机构提出投诉，并在以下情形下获得有效的司法救济：当数据主体认为其依据本指令所获条款享有的权利受到侵害；当监管机构未对投诉采取行动、部分或全部驳回投诉，或在保护数据主体权利必要时未采取行动。投诉调查应在司法审查框架下进行，且调查范围应根据具体案件情况适当调整。主管监管机构应在合理期限内向数据主体通报投诉进展及结果。若案件需进一步调查或与其他监管机构协调，应向数据主体提供阶段性信息。为便利投诉提交，各监管机构应采取相应措施，例如提供可电子填写的投诉提交表单，同时不排除其他沟通方式。

(86) 任何自然人或法人，若受到监管机构作出具有法律效力的决定，均应有权向本国主管法院寻求有效的司法救济。此类决定主要涉及监管机构行使调查权、纠正权及授权权，或驳回投诉等事项。但需注意，该权利不涵盖监管机构发布的非法律约束性意见或建议等措施。针对监管机构的诉讼，应向其设立地成员国法院提起，并依照该国法律进行审理。相关法院须行使充分管辖权，包括对案件中涉及的事实与法律问题进行审查的权限。

(87) 若数据主体认为其根据本指令享有的权利受到侵害，应有权委托专门机构，该机构旨在保护数据主体在相关事项中的权利与利益。

protection of their personal data and is constituted according to Member State law to lodge a complaint on his or her behalf with a supervisory authority and to exercise the right to a judicial remedy. The right of representation of data subjects should be without prejudice to Member State procedural law which may require mandatory representation of data subjects by a lawyer, as defined in Council Directive 77/249/EEC ([1]), before national courts.

(88) Any damage which a person may suffer as a result of processing that infringes the provisions adopted pursuant to this Directive should be compensated by the controller or any other authority competent under Member State law. 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 Directive. This is without prejudice to any claims for damage deriving from the violation of other rules in Union or Member State law. When reference is made to processing that is unlawful or that infringes the provisions adopted pursuant to this Directive it also covers processing that infringes implementing acts adopted pursuant to this Directive. Data subjects should receive full and effective compensation for the damage that they have suffered.

(89) Penalties should be imposed on any natural or legal person, whether governed by private or public law, who infringes this Directive. Member States should ensure that the penalties are effective, proportionate and dissuasive and should take all measures to implement the penalties.

(90) In order to ensure uniform conditions for the implementation of this Directive, implementing powers should be conferred on the Commission with regard to the adequate level of protection afforded by a third country, a territory or a specified sector within a third country, or an international organisation and the format and procedures for mutual assistance and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council ([2]).

(91) The examination procedure should be used for the adoption of implementing acts on the adequate level of protection afforded by a third country, a territory or a specified sector within a third country, or an international organisation and on the format and procedures for mutual assistance and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board, given that those acts are of a general scope.

(92) The Commission should adopt immediately applicable implementing acts where, in duly justified cases relating to a third country, a territory or a specified sector within a third country, or an international organisation which no longer ensure an adequate level of protection, imperative grounds of urgency so require.

(93) Since the objectives of this Directive, 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 exchange of personal data by competent authorities within 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 TEU. In accordance with the principle of proportionality as set out in that Article, this Directive does not go beyond what is necessary in order to achieve those objectives

(94) Specific provisions of acts of the Union adopted in the field of judicial cooperation in criminal matters and police cooperation which were adopted prior to the date of the adoption of this Directive, regulating the processing of personal data between Member States or the access of designated authorities of Member States to information

([1]) Council Directive 77/249/EEC of 22 March 1977 to facilitate the effective exercise by lawyers of freedom to provide services (OJ L 78, 26.3.1977, p. 17).

([2]) 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 the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

该机构依据成员国法律设立，负责保护数据主体的个人数据，代表其向监管机构提出投诉并行使司法救济权。数据主体的代理权应不影响成员国程序法的规定——根据欧盟理事会第77/249/EEC号指令（[1]）的定义，成员国法院在审理案件时可能要求必须由律师代表数据主体进行诉讼。

(88) 个人因违反本指令所规定条款的处理行为而遭受的任何损害，应由控制者或成员国法律授权的其他主管机构予以赔偿。损害赔偿的概念应结合欧洲法院判例法进行宽泛解释，以充分体现本指令的立法宗旨。此规定不影响因违反欧盟或成员国其他法律规则而产生的损害赔偿主张。当涉及非法处理或违反本指令条款的处理行为时，亦包括违反本指令所制定实施条例的情形。数据主体应获得充分有效的损害赔偿。

(89) 凡违反本指令的自然人或法人，无论适用私法或公法，均应予以处罚。各成员国须确保处罚措施切实有效、适度且具有威慑力，并应采取一切必要措施予以执行。

(90) 为确保本指令实施条件的统一性，应授权欧盟委员会行使以下职权：评估第三国、其领土或特定行业（或国际组织）提供的保护水平是否达标；制定监管机构间以及监管机构与欧盟委员会之间的电子化信息交换机制与程序。相关职权的行使须遵循欧洲议会和理事会第（EU）182/2011号条例（[2]）的规定。

(91) 鉴于这些行为具有普遍适用性，审查程序应适用于以下事项：就第三国、第三国境内特定领土或特定部门，或国际组织所提供的适当保护水平，以及监管机构之间、监管机构与委员会之间的相互协助形式、程序和通过电子手段交换信息的安排，通过实施性行为予以采纳。

(92) 若涉及第三国、第三国境内特定区域或特定行业，或国际组织的正当理由确需采取紧急措施，委员会应立即颁布可立即生效的实施条例。

(93) 鉴于本指令旨在保护自然人的基本权利与自由（特别是个人数据保护权）以及确保欧盟内部主管机构间个人数据自由交换的目标，若成员国无法充分实现这些目标，而鉴于该行动的规模或影响，可在欧盟层面更有效地达成，则欧盟可依据《欧盟条约》第5条规定的辅助性原则采取相应措施。根据该条款所确立的比例原则，本指令的实施范围不会超出实现上述目标所必需的限度。

(94) 在本指令颁布前已通过的欧盟刑事司法合作与警务合作领域法案中，有关成员国间个人数据处理或指定机构获取信息的具体规定

(1) 1977年3月22日理事会指令77/249/EEC，旨在促进律师有效行使提供服务的自由（OJ L 78， 26.3.1977 ，第17页）。

(2) 2011年2月16日欧洲议会和理事会第182/2011号条例，规定了关于成员国控制委员会行使实施权力的机制的规则和一般原则（OJ L 55， 28.2.2011 ，第13页）。

systems established pursuant to the Treaties, should remain unaffected, such as, for example, the specific provisions concerning the protection of personal data applied pursuant to Council Decision 2008/615/JHA ([1]), or Article 23 of the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union ([2]). Since Article 8 of the Charter and Article 16 TFEU require that the fundamental right to the protection of personal data be ensured in a consistent manner throughout the Union, the Commission should evaluate the situation with regard to the relationship between this Directive and the acts adopted prior to the date of adoption of this Directive regulating the processing of personal data between Member States or the access of designated authorities of Member States to information systems established pursuant to the Treaties, in order to assess the need for alignment of those specific provisions with this Directive. Where appropriate, the Commission should make proposals with a view to ensuring consistent legal rules relating to the processing of personal data.

(95) In order to ensure a comprehensive and consistent protection of personal data in the Union, international agreements which were concluded by Member States prior to the date of entry into force of this Directive and which comply with the relevant Union law applicable prior to that date should remain in force until amended, replaced or revoked.

(96) Member States should be allowed a period of not more than two years from the date of entry into force of this Directive to transpose it. Processing already under way on that date should be brought into conformity with this Directive within the period of two years after which this Directive enters into force. However, where such processing complies with the Union law applicable prior to the date of entry into force of this Directive, the requirements of this Directive concerning the prior consultation of the supervisory authority should not apply to the processing operations already under way on that date given that those requirements, by their very nature, are to be met prior to the processing. Where Member States use the longer implementation period expiring seven years after the date of entry into force of this Directive for meeting the logging obligations for automated processing systems set up prior to that date, the controller or the processor should have in place effective methods for demonstrating the lawfulness of the data processing, for enabling self-monitoring and for ensuring data integrity and data security, such as logs or other forms of records.

(97) This Directive is without prejudice to the rules on combating the sexual abuse and sexual exploitation of children and child pornography as laid down in Directive 2011/93/EU of the European Parliament and of the Council ([3]).

(98) Framework Decision 2008/977/JHA should therefore be repealed.

(99) In accordance with Article 6a of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, as annexed to the TEU and to the TFEU, the United Kingdom and Ireland are not bound by the rules laid down in this Directive which relate to the processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the TFEU where the United Kingdom and Ireland are not bound by the rules governing the forms of judicial cooperation in criminal matters or police cooperation which require compliance with the provisions laid down on the basis of Article 16 TFEU.

(100) In accordance with Articles 2 and 2a of Protocol No 22 on the position of Denmark, as annexed to the TEU and to the TFEU, Denmark is not bound by the rules laid down in this Directive or subject to their application which relate to the processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the TFEU. Given that this Directive builds upon the Schengen *acquis*, under Title V of Part Three of the TFEU, Denmark, in accordance with Article 4 of that Protocol, is to decide within six months after adoption of this Directive whether it will implement it in its national law.

(101) As regards Iceland and Norway, this Directive constitutes a development of provisions of the Schengen *acquis*, as provided for by the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen *acquis* ([4]).

([1]) Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (OJ L 210, 6.8.2008, p. 1).

([2]) Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (OJ C 197, 12.7.2000, p. 1).

([3]) Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ L 335, 17.12.2011, p. 1).

([4]) OJ L 176, 10.7.1999, p. 36.

根据条约建立的系统应不受影响，例如，根据理事会决定2008/615/ JHA（[1]）或《欧洲联盟成员国间刑事事项互助公约》第23条（[2]）所适用的关于个人数据保护的具体规定。由于《宪章》第8条和第16条TFEU 要求在整个联盟内以一致的方式确保个人数据保护的基本权利，委员会应评估本指令与在本指令通过前已采取的、规范成员国间个人数据处理或成员国指定当局访问根据条约建立的信息系统的措施之间的关系，以评估这些特定规定与本指令协调的必要性。在适当情况下，委员会应提出建议，以确保与个人数据处理相关的法律规则的一致性。

(95) 为确保欧盟境内个人数据获得全面且一致的保护，各成员国在本指令生效前签署的、符合该日期前适用的欧盟相关法律的国际协议，应维持原有效力直至被修订、取代或废止。

(96) 各成员国应获准在本指令生效之日起两年内完成其转化工作。对于在该日期已启动的数据处理活动，应在本指令生效后的两年内完成合规调整。但若相关处理活动符合本指令生效前适用的欧盟法律，则本指令关于事先征询监管机构意见的要求，不适用于该日期已开展的数据处理业务——因为这些要求本质上需在处理活动启动前就已满足。若成员国采用更长的七年实施期来履行对本指令生效前建立的自动化处理系统进行日志记录的义务，则数据控制者或处理者应建立有效机制，通过日志或其他记录形式证明数据处理的合法性，实现自我监管，并确保数据完整性和安全性。

(97) 本指令不影响欧洲议会和欧洲理事会第2011/93/EU号指令中关于打击性虐待和性剥削儿童及儿童色情制品的规定（[3]）。

(98) 因此，应废除第2008/977/ JHA 号框架决定。

(99) 根据《欧洲联盟条约》和《欧洲联盟运作条约》附件中关于英国和爱尔兰在自由、安全与正义领域立场的第21号议定书第6a条，英国和爱尔兰不受本指令中关于成员国在执行《欧洲联盟运作条约》第三部分第五章第四章或第五章所涵盖活动时处理个人数据的规则约束，即英国和爱尔兰不受《欧洲联盟运作条约》第16条规定的刑事司法合作或警察合作形式规则的约束。

(100) 根据《欧盟运行条约》和《通用数据保护条例》（TFEU）所附的第22号议定书第2条及第2a条之规定，丹麦在执行属于 TFEU 第三部分第五章第四章或第五章范围内的活动时，不受该指令所制定的或适用的关于成员国处理个人数据的规则约束。鉴于本指令建立在《申根*法规*》基础之上，根据该议定书第4条规定，丹麦应在本指令通过后六个月内决定是否将其纳入本国法律。

(101) 关于冰岛和挪威，本指令是*欧洲联盟理事会与冰岛共和国和挪威王国就这两个国家加入沙根 体系*的执行、适用和发展所缔结的协定中所载*沙根体系*条款的进一步发展。

---

(1) 2008年6月23日关于加强跨境合作，特别是打击恐怖主义和跨境犯罪的理事会决定2008/615/ JHA（OJ L 210,2008年8月6日，第1页）。

(2) 2000年5月29日根据《欧洲联盟条约》第34条设立的欧洲联盟成员国间刑事事项互助公约理事会法案（OJ C 197，12.7.2000，第1页）。

(3) 欧洲议会和理事会2011年12月13日关于打击对儿童的性虐待和性剥削以及儿童色情制品的第2011/93/EU号指令，以及取代理事会第2004/68/ JHA 号框架决定（OJ L 335， 17.12.2011，第1页）。

(4) OJ L 176, 10.7.1999, p. 36.

(102) As regards Switzerland, this Directive constitutes a development of provisions of the Schengen *acquis*, as provided for by the Agreement between the European Union, the European Community and the Swiss Confederation concerning the association of the Swiss Confederation with the implementation, application and development of the Schengen *acquis* ([1]).

(103) As regards Liechtenstein, this Directive constitutes a development of provisions of the Schengen *acquis*, as provided for by the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* ([2]).

(104) This Directive respects the fundamental rights and observes the principles recognised in the Charter as enshrined in the TFEU, in particular the right to respect for private and family life, the right to the protection of personal data, the right to an effective remedy and to a fair trial. Limitations placed on those rights are in accordance with Article 52(1) of the Charter as they are necessary to meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

(105) In accordance with the Joint Political Declaration of 28 September 2011 of Member States and the Commission on explanatory documents, Member States have undertaken to accompany, in justified cases, the notification of their transposition measures with one or more documents explaining the relationship between the components of a directive and the corresponding parts of national transposition measures. With regard to this Directive, the legislator considers the transmission of such documents to be justified.

(106) 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 ([3]).

(107) This Directive should not preclude Member States from implementing the exercise of the rights of data subjects on information, access to and rectification or erasure of personal data and restriction of processing in the course of criminal proceedings, and their possible restrictions thereto, in national rules on criminal procedure,

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I

General provisions

Article 1

Subject-matter and objectives

1. This Directive lays down the rules relating to 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.

2. In accordance with this Directive, Member States shall:

(a) protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data; and

(b) ensure that the exchange of personal data by competent authorities within the Union, where such exchange is required by Union or Member State law, is neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

([1]) OJ L 53, 27.2.2008, p. 52.
([2]) OJ L 160, 18.6.2011, p. 21.
([3]) OJ C 192, 30.6.2012, p. 7.

(102) 关于瑞士，该指令是*欧洲联盟、欧洲共同体和瑞士联邦之间关于瑞士联邦加入执行、适用和制定沙根成果*的协定所载的*沙根成果*规定的进一步发展。

(103) 关于列支敦士登，该指令是*欧洲联盟、欧洲共同体、瑞士联邦和列支敦士登公国之间关于列支敦士登公国加入欧洲联盟、欧洲共同体和瑞士联邦之间关于瑞士联邦加入执行、适用和制定沙根 成果*的协定的议定书所载的*沙根成果*规定的进一步发展。

(104) 本指令尊重基本权利并遵守《宪章》中确立的原则，特别是《欧洲人权公约》（TFEU）中规定的尊重私人和家庭生活、保护个人数据、获得有效救济和公正审判的权利。对这些权利的限制符合《宪章》第52条第1款的规定，因为这些限制对于实现联盟认可的公共利益目标或保护他人权利和自由是必要的。

(105) 根据成员国2011年9月28日联合政治宣言及委员会关于解释性文件的说明，成员国承诺在合理情况下，随其转置措施通知附上一份或多份文件，阐明指令各组成部分与国家转置措施对应部分之间的关系。针对本指令，立法者认为提交此类文件是合理的。

(106) 根据第（EC）45/2001号条例第28(2)条的规定，咨询了欧洲数据保护监督员，并于2012年3月7日提交了意见书（[3]）。

(107) 本指令不应妨碍成员国在刑事诉讼程序中，通过国内刑事诉讼规则，落实数据主体关于信息获取、个人数据访问与更正或删除以及数据处理限制的权利，以及可能施加的限制。

已通过本指令：

第一章

一般规定

第1条

研究主题与目的

1. 本指令规定了主管当局为预防、调查、侦查或起诉刑事犯罪，或执行刑事处罚（包括维护公共安全）而处理个人数据时对自然人保护的相关规则。

2. 根据该指令，成员国应：

(a) 保护自然人的基本权利和自由，特别是其个人数据保护权；

(b) 确保欧盟境内主管当局在欧盟或成员国法律要求下交换个人数据时，不得以保护自然人在个人数据处理方面权益为由限制或禁止此类交换。

([1]) OJ L 53, 27.2.2008, p. 52.
([2]) OJ L 160, 18.6.2011, p. 21.
([3]) OJ C 192, 30.6.2012, p. 7.

3. This Directive shall not preclude Member States from providing higher safeguards than those established in this Directive for the protection of the rights and freedoms of the data subject with regard to the processing of personal data by competent authorities.

Article 2

Scope

1. This Directive applies to the processing of personal data by competent authorities for the purposes set out in Article 1(1).

2. This Directive 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.

3. This Directive 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 Union institutions, bodies, offices and agencies.

Article 3

Definitions

For the purposes of this Directive:

(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) 'competent authority' means:

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

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

3. 本指令不妨碍各成员国在主管当局处理个人数据时，为数据主体的权利和自由提供高于本指令所规定的保障措施。

第2条

范围

1. 本指令适用于主管当局为实现第1条第1款所列目的而进行的个人数据处理。

2. 本指令适用于以下情形：通过自动化手段全部或部分处理个人数据，以及非自动化手段处理构成或拟构成备案系统组成部分的个人数据。

3. 本指令不适用于个人数据的处理：

(a) 在涉及欧盟法律范围之外的活动过程中；

(b) 由联邦机构、部门、办公室及下属单位负责。

第3条

定义

本指令所指：

(1) ‘个人数据’指与已识别或可识别的自然人（‘数据主体’）相关的任何信息；可识别的自然人是指可通过直接或间接方式识别的自然人，特别是通过姓名、识别号码、位置数据、在线标识符或该自然人在生理、遗传、心理、经济、文化或社会身份方面的一个或多个特定因素来识别的自然人；

(2) ‘处理’指对个人数据或个人数据集实施的任何操作或操作组合，无论是否通过自动化手段，包括但不限于：收集、记录、组织、结构化、存储、调整或修改、检索、查阅、使用、通过传输或传播方式披露、对齐或组合、限制、删除或销毁等。

(3) “限制处理”是指对存储的个人数据进行标记，旨在限制其未来的处理；

(4) ‘个人画像’指通过自动化处理个人数据，评估自然人特定个人特征的行为，具体包括分析或预测其工作表现、经济状况、健康状况、个人偏好、兴趣、可信度、行为模式、地理位置及活动轨迹等信息。

(5) ‘匿名化’指对个人数据进行处理，使其无法在缺乏额外信息的情况下追溯至特定数据主体，前提是这些额外信息需单独保存，并通过技术及组织措施确保个人数据不会被追溯至已识别或可识别的自然人。

(6) ‘归档系统’指根据特定标准可访问的任何结构化个人数据集合，无论其是集中式、分散式，还是基于功能或地理分布的分散式；

(7) “主管机关”是指：

(a) 任何有权预防、调查、侦查或起诉刑事犯罪或执行刑事处罚的公共权力机关，包括维护和预防公共安全威胁的公共权力机关；

(b) 根据成员国法律授权，任何其他机构或实体可行使公共权力与职权，以预防、调查、侦办或起诉刑事犯罪，执行刑事处罚，包括维护公共安全及防范相关威胁。

(8) 'controller' means the competent authority 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;

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

(10) '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 framework of a particular inquiry in accordance with 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;

(11) '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;

(12) '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;

(13) '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;

(14) '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;

(15) 'supervisory authority' means an independent public authority which is established by a Member State pursuant to Article 41;

(16) '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 4

Principles relating to processing of personal data

1. Member States shall provide for personal data to be:

(a) processed lawfully and fairly;

(b) collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes;

(c) adequate, relevant and not excessive in relation to the purposes for which they are processed;

(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;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed;

(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.

(8) ‘控制者’指单独或联合其他主体确定个人数据处理目的及方式的主管机关；若该处理目的及方式由欧盟或成员国法律确定，则控制者或其指定的具体标准可由欧盟或成员国法律予以规定。

(9) “处理者”指代表控制者处理个人数据的自然人或法人、公共机构、代理机构或其他实体；

(10) ‘接收方’指自然人或法人、公共机构、代理机构或其他实体，无论是否为第三方，均视为个人数据的接收方。但根据成员国法律，在特定调查框架下可能接收个人数据的公共机构不被视为接收方；此类公共机构对数据的处理应符合适用的数据保护规则，并与处理目的相符。

(11) “个人数据泄露”指因安全措施缺失，导致传输、存储或处理的个人数据发生意外或非法损毁、丢失、篡改、未经授权披露或被非法获取的行为；

(12) ‘遗传数据’指与自然人遗传或获得性遗传特征相关的个人数据，这些数据能提供该自然人生理或健康状况的独特信息，且主要来源于对该自然人生物样本的分析；

(13) ‘生物特征数据’指通过特定技术处理获得的个人数据，这些数据涉及自然人的生理、行为或体征特征，可实现该自然人的唯一识别，例如面部图像或指纹数据。

(14) “健康相关数据”指与自然人身心健康相关的个人数据，包括提供医疗服务时所披露的健康状况信息；

(15) ‘监督机构’指成员国根据第41条设立的独立公共机构；

(16) “国际组织”指受国际公法管辖的组织及其下属机构，或由两个以上国家根据协议设立的任何其他机构。

第II章

原则

第4条

个人数据处理相关原则

1. 成员国应确保个人数据：

(a) 依法公正处理；

(b) 为明确、具体且合法的目的收集，并且处理方式不违背这些目的；

(c) 与处理目的相关且不过度的充分性；

(d) 准确且必要时及时更新；必须采取一切合理措施，确保与处理目的相关的不准确个人数据立即被删除或更正；

(e) 以允许识别数据主体的形式保存，保存时间不得超过其处理目的所需的必要期限；

(f) 以确保个人数据安全的方式进行处理，包括采取适当的技术或组织措施，防止未经授权或非法处理，以及防止意外丢失、破坏或损坏。

2. Processing by the same or another controller for any of the purposes set out in Article 1(1) other than that for which the personal data are collected shall be permitted in so far as:

(a) the controller is authorised to process such personal data for such a purpose in accordance with Union or Member State law; and

(b) processing is necessary and proportionate to that other purpose in accordance with Union or Member State law.

3. Processing by the same or another controller may include archiving in the public interest, scientific, statistical or historical use, for the purposes set out in Article 1(1), subject to appropriate safeguards for the rights and freedoms of data subjects.

4. The controller shall be responsible for, and be able to demonstrate compliance with, paragraphs 1, 2 and 3.

Article 5

Time-limits for storage and review

Member States shall provide for appropriate time limits to be established for the erasure of personal data or for a periodic review of the need for the storage of personal data. Procedural measures shall ensure that those time limits are observed.

Article 6

Distinction between different categories of data subject

Member States shall provide for the controller, where applicable and as far as possible, to make a clear distinction between personal data of different categories of data subjects, such as:

(a) persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence;

(b) persons convicted of a criminal offence;

(c) victims of a criminal offence or persons with regard to whom certain facts give rise to reasons for believing that he or she could be the victim of a criminal offence; and

(d) other parties to a criminal offence, such as persons who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings, persons who can provide information on criminal offences, or contacts or associates of one of the persons referred to in points (a) and (b).

Article 7

Distinction between personal data and verification of quality of personal data

1. Member States shall provide for personal data based on facts to be distinguished, as far as possible, from personal data based on personal assessments.

2. Member States shall provide for the competent authorities to take all reasonable steps to ensure that personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available. To that end, each competent authority shall, as far as practicable, verify the quality of personal data before they are transmitted or made available. As far as possible, in all transmissions of personal data, necessary information enabling the receiving competent authority to assess the degree of accuracy, completeness and reliability of personal data, and the extent to which they are up to date shall be added.

3. If it emerges that incorrect personal data have been transmitted or personal data have been unlawfully transmitted, the recipient shall be notified without delay. In such a case, the personal data shall be rectified or erased or processing shall be restricted in accordance with Article 16.

2. 若处理目的符合第1条第1款规定（但不包括收集个人数据的用途），则允许由同一或另一控制者进行处理，前提是：

(a) 数据控制者有权依据欧盟或成员国法律，为上述目的处理此类个人数据；且

(b) 处理应符合欧盟或成员国法律，且与该其他目的相称。

3. 同一或另一控制者进行的处理，可包括出于公共利益、科学、统计或历史用途而进行的归档，具体目的如第1条第1款所述，但须对数据主体的权利和自由采取适当保障措施。

4. 该控制器应负责并能够证明其符合第1、2和3段的规定。

第5条

储存和审查时限

各成员国应规定适当的时间限制，用于删除个人数据或定期审查存储个人数据的必要性。程序性措施应确保遵守这些时间限制。

第6条

区分不同类别的数据主体

成员国应确保数据控制者在适用情况下尽可能明确区分不同类别数据主体的个人数据，例如：

(a) 有充分理由认为其已实施或即将实施刑事犯罪的人员；

(b) 被定罪的刑事犯罪者；

(c) 刑事犯罪的受害者或因某些事实而有理由认为可能成为刑事犯罪受害者的人员；以及

(d) 其他刑事犯罪相关方，包括可能被传唤参与刑事犯罪调查或后续刑事诉讼作证的人员、能够提供犯罪信息的人员，以及(a)和(b)项所述人员的联系人或关联方。

第7条

个人数据的区分与个人数据质量的验证

1. 成员国应确保基于事实的个人数据尽可能与基于个人评估的个人数据相区分。

2. 成员国应确保主管机构采取一切合理措施，防止不准确、不完整或已过期的个人数据被传输或公开。为此，各主管机构应在可行范围内，对个人数据进行传输或公开前的质量核查。在所有个人数据传输过程中，应尽可能提供必要信息，以便接收方主管机构评估数据的准确性、完整性、可靠性及时效性。

3. 若发现传输的个人数据存在错误或非法传输，应立即通知接收方。在此情况下，应依据第16条规定对个人数据进行更正、删除或限制处理。

Article 8

Lawfulness of processing

1. Member States shall provide for processing to be lawful only if and to the extent that processing is necessary for the performance of a task carried out by a competent authority for the purposes set out in Article 1(1) and that it is based on Union or Member State law.

2. Member State law regulating processing within the scope of this Directive shall specify at least the objectives of processing, the personal data to be processed and the purposes of the processing.

Article 9

Specific processing conditions

1. Personal data collected by competent authorities for the purposes set out in Article 1(1) shall not be processed for purposes other than those set out in Article 1(1) unless such processing is authorised by Union or Member State law. Where personal data are processed for such other purposes, Regulation (EU) 2016/679 shall apply unless the processing is carried out in an activity which falls outside the scope of Union law.

2. Where competent authorities are entrusted by Member State law with the performance of tasks other than those performed for the purposes set out in Article 1(1), Regulation (EU) 2016/679 shall apply to processing for such purposes, including for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, unless the processing is carried out in an activity which falls outside the scope of Union law.

3. Member States shall, where Union or Member State law applicable to the transmitting competent authority provides specific conditions for processing, provide for the transmitting competent authority to inform the recipient of such personal data of those conditions and the requirement to comply with them.

4. Member States shall provide for the transmitting competent authority not to apply conditions pursuant to paragraph 3 to recipients in other Member States or to agencies, offices and bodies established pursuant to Chapters 4 and 5 of Title V of the TFEU other than those applicable to similar transmissions of data within the Member State of the transmitting competent authority.

Article 10

Processing of special categories of personal data

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 allowed only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only:

(a) where authorised by Union or Member State law;

(b) to protect the vital interests of the data subject or of another natural person; or

(c) where such processing relates to data which are manifestly made public by the data subject.

Article 11

Automated individual decision-making

1. Member States shall provide for a decision based solely on automated processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her, to be prohibited unless authorised by Union or Member State law to which the controller is subject and which provides appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller.

第8条

加工合法性

1. 成员国须确保数据处理合法，前提是该处理对于主管机关执行第1条第1款所列任务确有必要，且基于欧盟或成员国法律。

2. 成员国法律在规范本指令范围内的数据处理时，应至少规定处理目的、拟处理的个人数据及处理目的。

第9条

特定加工条件

1. 主管当局为实现第1条第1款所列目的而收集的个人数据，除非获得欧盟或成员国法律授权，否则不得用于其他目的。若个人数据被用于其他目的，应适用欧盟第2016/679号条例，除非该处理属于欧盟法律管辖范围之外的活动。

2. 当成员国法律授权主管机关执行第1条第1款规定之外的任务时，欧盟第2016/679号条例应适用于此类目的的数据处理，包括出于公共利益、科学研究或历史研究目的以及统计目的的归档目的，除非该处理活动属于欧盟法律范围之外的范畴。

3. 若欧盟或成员国法律对传输主管机关规定了特定处理条件，成员国应确保该主管机关向接收方告知相关条件及合规要求。

4. 成员国应规定，发送主管机关不得对其他成员国的接收方或对根据 TFEU 第五章第4和第5章设立的机构、办公室和机构适用第3款规定的条件，但适用于发送主管机关成员国境内类似数据传输的条件除外。

第10条

特殊类别个人数据的处理

处理涉及种族或民族起源、政治观点、宗教或哲学信仰或工会成员身份的个人数据，以及处理用于唯一识别自然人的基因数据、生物识别数据、健康数据或自然人性生活或性取向数据，仅在严格必要时允许，且须对数据主体的权利和自由采取适当保障措施，且仅限于：

(a) 经欧盟或成员国法律授权；

(b) 保护数据主体或其他自然人的合法权益；或

(c) 当此类处理涉及数据主体已明确公开的数据时。

第11条

自动化个体决策

1. 成员国应规定，除非欧盟或控制者所适用的成员国法律授权，并为数据主体的权利和自由提供适当保障（至少包括控制者进行人工干预的权利），否则禁止仅基于自动化处理（包括画像分析）而产生的、对数据主体产生不利法律后果或对其造成重大影响的决定。

2. Decisions referred to in paragraph 1 of this Article shall not be based on special categories of personal data referred to in Article 10, unless suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

3. Profiling that results in discrimination against natural persons on the basis of special categories of personal data referred to in Article 10 shall be prohibited, in accordance with Union law.

CHAPTER III

Rights of the data subject

Article 12

Communication and modalities for exercising the rights of the data subject

1. Member States shall provide for the controller to take reasonable steps to provide any information referred to in Article 13 and make any communication with regard to Articles 11, 14 to 18 and 31 relating to processing to the data subject in a concise, intelligible and easily accessible form, using clear and plain language. The information shall be provided by any appropriate means, including by electronic means. As a general rule, the controller shall provide the information in the same form as the request.

2. Member States shall provide for the controller to facilitate the exercise of the rights of the data subject under Articles 11 and 14 to 18.

3. Member States shall provide for the controller to inform the data subject in writing about the follow up to his or her request without undue delay.

4. Member States shall provide for the information provided under Article 13 and any communication made or action taken pursuant to Articles 11, 14 to 18 and 31 to 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.

5. Where the controller has reasonable doubts concerning the identity of the natural person making a request referred to in Article 14 or 16, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

Article 13

Information to be made available or given to the data subject

1. Member States shall provide for the controller to make available to the data subject at least the following information:

(a) the identity and the contact details of the controller;

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

(c) the purposes of the processing for which the personal data are intended;

(d) the right to lodge a complaint with a supervisory authority and the contact details of the supervisory authority;

(e) the existence of the right to request from the controller access to and rectification or erasure of personal data and restriction of processing of the personal data concerning the data subject.

2. In addition to the information referred to in paragraph 1, Member States shall provide by law for the controller to give to the data subject, in specific cases, the following further information to enable the exercise of his or her rights:

(a) the legal basis for the processing;

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

2. 本条第1款所述决定不得基于第10条所列的特殊个人数据类别，除非已采取适当措施保障数据主体的权利、自由及合法权益。

3. 根据欧盟法律，基于第10条所列特定个人数据类别而对自然人实施的歧视性个人资料分析应被禁止。

第III章

数据主体的权利

第12条

行使数据主体权利的沟通方式与模式

1. 各成员国应确保数据控制者采取合理措施，以清晰易懂且便于获取的形式，使用通俗易懂的语言，向数据主体提供第13条所述信息，并就第11条、第14至18条及第31条涉及数据处理的相关事项进行沟通。相关信息应通过适当方式提供，包括电子方式。一般而言，数据控制者应以与请求相同的形式提供信息。

2. 各成员国应确保数据控制者能够便利数据主体根据第11条及第14至18条行使权利。

3. 成员国应确保数据控制者以书面形式及时告知数据主体其请求的后续处理情况，不得无故拖延。

4. 各成员国应确保第13条所载信息以及依据第11条、第14至18条和第31条所作的任何沟通或采取的行动均免费提供。若数据主体的请求明显缺乏依据或过度，特别是因其重复性，控制者可采取以下措施：

(a) 收取合理费用，同时考虑提供信息或通信或采取所要求行动所产生的行政成本；或

(b) 拒绝执行请求。

控制方须承担举证责任，证明该请求明显缺乏依据或存在过度性。

5. 若控制者对第14条或第16条所述自然人身份存有合理疑问，可要求提供确认数据主体身份所需的补充信息。

第十三条

需向数据主体提供或提供的信息

1. 成员国应确保控制者向数据主体提供至少以下信息：

(a) 控制者的身份及联系方式；

(b) 如适用，提供数据保护官的联系方式；

(c) 个人数据处理的目的；

(d) 向监管机构提出投诉的权利及监管机构的联系方式；

(e) 数据主体享有向控制者请求访问、更正或删除个人数据的权利，以及限制处理其个人数据的权利。

2. 除第1款所述信息外，各成员国应通过立法规定，数据控制者在特定情况下须向数据主体提供以下补充信息，以保障其权利的行使：

(a) 处理的法律依据；

(b) 个人数据的存储期限，或在无法确定存储期限时，用于确定该期限的标准；

(c) where applicable, the categories of recipients of the personal data, including in third countries or international organisations;

(d) where necessary, further information, in particular where the personal data are collected without the knowledge of the data subject.

3. Member States may adopt legislative measures delaying, restricting or omitting the provision of the information to the data subject pursuant to paragraph 2 to the extent that, and for as long as, such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned, in order to:

(a) avoid obstructing official or legal inquiries, investigations or procedures;

(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

(c) protect public security;

(d) protect national security;

(e) protect the rights and freedoms of others.

4. Member States may adopt legislative measures in order to determine categories of processing which may wholly or partly fall under any of the points listed in paragraph 3.

Article 14

Right of access by the data subject

Subject to Article 15, Member States shall provide for the right of the data subject 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 and legal basis for the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipients to whom the personal data have been 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;

(f) the right to lodge a complaint with the supervisory authority and the contact details of the supervisory authority;

(g) communication of the personal data undergoing processing and of any available information as to their origin.

Article 15

Limitations to the right of access

1. Member States may adopt legislative measures restricting, wholly or partly, the data subject's right of access to the extent that, and for as long as such a partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned, in order to:

(a) avoid obstructing official or legal inquiries, investigations or procedures;

(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

(c) protect public security;

(c) 在适用情况下，个人数据接收方的类别，包括位于第三国或国际组织的接收方；

(d) 必要时，需提供进一步信息，特别是当个人数据在数据主体不知情的情况下被收集时。

3. 成员国可采取立法措施，延迟、限制或免除向数据主体提供第2款所规定信息的义务，但须满足以下条件：在充分尊重相关自然人基本权利和合法权益的前提下，该措施须符合民主社会的必要性与相称性原则，且仅在必要且持续适用的范围内实施。

(a) 不得妨碍官方或法律调查、调查或程序；

(b) 不得妨碍刑事犯罪的预防、侦查、侦查或起诉，或妨碍刑事处罚的执行；

(c) 保护公共安全；

(d) 保护国家安全；

(e) 保护他人的权利和自由。

4. 成员国可采取立法措施，以确定哪些数据处理类别可能全部或部分属于第3段所列任一情形。

第14条

数据主体的访问权

根据第15条规定，各成员国应保障数据主体有权要求数据控制者确认是否正在处理其个人数据；若确有处理，数据主体还应有权查阅相关个人数据及以下信息：

(a) 处理的目的及法律依据；

(b) 所涉个人数据类别；

(c) 个人数据的接收方或接收类别，特别是第三国或国际组织的接收方；

(d) 如有可能，应注明个人数据预期存储期限；若无法确定，则应说明确定该期限所依据的标准。

(e) 数据主体有权要求控制者更正或删除其个人数据，或限制对个人数据的处理；

(f) 向监管机构提出投诉的权利及监管机构的联系方式；

(g) 关于正在处理的个人数据及其来源信息的披露。

第15条

访问权的限制

1. 成员国可采取立法措施，对数据主体的访问权实施全部或部分限制，但须满足以下条件：在充分尊重相关自然人基本权利与合法利益的前提下，此类限制在民主社会中构成必要且相称的措施，并持续适用。

(a) 不得妨碍官方或法律调查、调查或程序；

(b) 不得妨碍刑事犯罪的预防、侦查、侦查或起诉，或妨碍刑事处罚的执行；

(c) 保护公共安全；

(d) protect national security;

(e) protect the rights and freedoms of others.

2. Member States may adopt legislative measures in order to determine categories of processing which may wholly or partly fall under points (a) to (e) of paragraph 1.

3. In the cases referred to in paragraphs 1 and 2, Member States shall provide for the controller to inform the data subject, without undue delay, in writing of any refusal or restriction of access and of the reasons for the refusal or the restriction. Such information may be omitted where the provision thereof would undermine a purpose under paragraph 1. Member States shall provide for the controller to inform the data subject of the possibility of lodging a complaint with a supervisory authority or seeking a judicial remedy.

4. Member States shall provide for the controller to document the factual or legal reasons on which the decision is based. That information shall be made available to the supervisory authorities.

Article 16

Right to rectification or erasure of personal data and restriction of processing

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

2. Member States shall require the controller to erase personal data without undue delay and provide for the right of the data subject to obtain from the controller the erasure of personal data concerning him or her without undue delay where processing infringes the provisions adopted pursuant to Article 4, 8 or 10, or where personal data must be erased in order to comply with a legal obligation to which the controller is subject.

3. Instead of erasure, the controller shall restrict processing where:

(a) the accuracy of the personal data is contested by the data subject and their accuracy or inaccuracy cannot be ascertained; or

(b) the personal data must be maintained for the purposes of evidence.

Where processing is restricted pursuant to point (a) of the first subparagraph, the controller shall inform the data subject before lifting the restriction of processing.

4. Member States shall provide for the controller to inform the data subject in writing of any refusal of rectification or erasure of personal data or restriction of processing and of the reasons for the refusal. Member States may adopt legislative measures restricting, wholly or partly, the obligation to provide such information to the extent that such a restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned in order to:

(a) avoid obstructing official or legal inquiries, investigations or procedures;

(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

(c) protect public security;

(d) protect national security;

(e) protect the rights and freedoms of others.

Member States shall provide for the controller to inform the data subject of the possibility of lodging a complaint with a supervisory authority or seeking a judicial remedy.

(d) 保护国家安全；

(e) 保护他人的权利和自由。

2. 成员国可采取立法措施，以确定哪些数据处理类别可能全部或部分属于第1款(a)至(e)项。

3. 对于第1款和第2款所述情形，成员国应规定数据控制者须以书面形式及时告知数据主体任何访问权限的拒绝或限制，并说明拒绝或限制的理由。若提供此类信息可能损害第1款所述目的，则可予以省略。成员国还应规定数据控制者须告知数据主体可向监管机构提出投诉或寻求司法救济。

4. 成员国应要求控制者记录该决定所依据的事实或法律依据。该信息应向监管机构提供。

第16条

个人数据更正或删除权及处理限制

1. 各成员国应保障数据主体有权要求控制者及时更正与其相关的不准确个人数据。考虑到数据处理目的，各成员国应保障数据主体有权要求补充不完整的个人数据，包括通过提供补充声明的方式。

2. 成员国应要求控制者在处理数据时不得无故延迟删除个人数据，并规定数据主体有权要求控制者在以下情况下立即删除其个人数据：处理行为违反第4条、第8条或第10条所规定的条款；或为履行控制者所承担的法律义务而必须删除个人数据。

3. 控制器应限制处理而非清除，具体情形包括：

(a) 数据主体对个人数据的准确性提出异议，且无法确认其准确性或不准确性；或

(b) 个人数据必须为证据目的而保存。

若依据第一款(a)项规定处理受到限制，控制者应在解除处理限制前通知数据主体。

4. 成员国应规定，数据控制者须以书面形式向数据主体告知拒绝更正或删除个人数据、限制数据处理的决定及其理由。成员国可采取立法措施，对提供此类信息的义务进行全部或部分限制，但须确保此类限制在充分考虑相关自然人的基本权利和合法权益的前提下，构成民主社会中必要且相称的措施，以实现以下目的：

(a) 不得妨碍官方或法律调查、调查或程序；

(b) 不得妨碍刑事犯罪的预防、侦查、侦查或起诉，或妨碍刑事处罚的执行；

(c) 保护公共安全；

(d) 保护国家安全；

(e) 保护他人的权利和自由。

成员国应确保数据控制者向数据主体告知可向监管机构提出投诉或寻求司法救济的可能性。

5. Member States shall provide for the controller to communicate the rectification of inaccurate personal data to the competent authority from which the inaccurate personal data originate.

6. Member States shall, where personal data has been rectified or erased or processing has been restricted pursuant to paragraphs 1, 2 and 3, provide for the controller to notify the recipients and that the recipients shall rectify or erase the personal data or restrict processing of the personal data under their responsibility.

Article 17

Exercise of rights by the data subject and verification by the supervisory authority

1. In the cases referred to in Article 13(3), Article 15(3) and Article 16(4) Member States shall adopt measures providing that the rights of the data subject may also be exercised through the competent supervisory authority.

2. Member States shall provide for the controller to inform the data subject of the possibility of exercising his or her rights through the supervisory authority pursuant to paragraph 1.

3. Where the right referred to in paragraph 1 is exercised, the supervisory authority shall inform the data subject at least that all necessary verifications or a review by the supervisory authority have taken place. The supervisory authority shall also inform the data subject of his or her right to seek a judicial remedy.

Article 18

Rights of the data subject in criminal investigations and proceedings

Member States may provide for the exercise of the rights referred to in Articles 13, 14 and 16 to be carried out in accordance with Member State law where the personal data are contained in a judicial decision or record or case file processed in the course of criminal investigations and proceedings.

CHAPTER IV

Controller and processor

Section 1

General obligations

Article 19

Obligations of the controller

1. Member States shall provide for the controller, 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, to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Directive. Those measures shall be reviewed and updated where necessary.

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

Article 20

Data protection by design and by default

1. Member States shall provide for the controller, 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, both at the time of the determination of the means for processing and at the time of the processing itself, to 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 Directive and protect the rights of data subjects.

5. 成员国应规定数据控制者向数据不准确的来源主管机关通报不准确个人数据的更正情况。

6. 当个人数据依据第1、2、3款规定完成更正或删除，或其处理受到限制时，成员国应确保控制者向接收方发出通知，接收方须在其职责范围内完成数据更正或删除，或限制相关数据的处理。

第17条

数据主体行使权利与监管机构的核查

1. 对于第13条第3款、第15条第3款及第16条第4款所列情形，各成员国应制定相应措施，规定数据主体亦可通过主管监管机构行使权利。

2. 各成员国应确保数据控制者向数据主体告知，其可通过第1款规定的监督机构行使权利。

3. 当行使第1款所述权利时，监管机构应至少告知数据主体，所有必要的核查或监管机构的审查均已完成。监管机构还应告知数据主体其寻求司法救济的权利。

第18条

刑事侦查和诉讼中数据主体的权利

成员国可规定，当个人数据包含在刑事调查及诉讼过程中处理的司法裁决、记录或案卷中时，第13条、第14条及第16条所涉权利的行使应依据成员国法律进行。

第四章

控制器和处理机

第1节

一般性义务

第十九条

控制器的义务

1. 各成员国应要求数据控制者，综合考量数据处理的性质、范围、背景及目的，以及对自然人权利与自由可能产生的不同风险程度与严重性，采取适当的技术和组织措施，确保数据处理符合本指令要求，并能证明其合规性。相关措施应根据需要进行审查和更新。

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。

第二十条

设计和默认数据保护

1. 各成员国应要求数据控制者在确定数据处理方式及实际处理过程中，充分考虑技术发展水平、实施成本、数据处理的性质、范围、背景及目的，以及数据处理可能对自然人权利和自由造成的可能性与严重程度差异的风险，采取适当的技术和组织措施（如匿名化处理），有效落实数据最小化等数据保护原则，并将必要保障措施纳入数据处理流程，以满足本指令要求并保护数据主体权利。

2. Member States shall provide for the controller to implement appropriate technical and organisational measures 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.

Article 21

Joint controllers

1. Member States shall, where two or more controllers jointly determine the purposes and means of processing, provide for them to be joint controllers. They shall, in a transparent manner, determine their respective responsibilities for compliance with this Directive, in particular as regards the exercise of the rights of the data subject and their respective duties to provide the information referred to in Article 13, 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 shall designate the contact point for data subjects. Member States may designate which of the joint controllers can act as a single contact point for data subjects to exercise their rights.

2. Irrespective of the terms of the arrangement referred to in paragraph 1, Member States may provide for the data subject to exercise his or her rights under the provisions adopted pursuant to this Directive in respect of and against each of the controllers.

Article 22

Processor

1. Member States shall, where processing is to be carried out on behalf of a controller, provide for the controller to use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Directive and ensure the protection of the rights of the data subject.

2. Member States shall provide for the processor not to engage another processor without prior specific or general written authorisation by 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. Member States shall provide for the processing by a processor to 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) acts only on instructions from the controller;

(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) assists the controller by any appropriate means to ensure compliance with the provisions on the data subject's rights;

(d) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of data processing services, and deletes existing copies unless Union or Member State law requires storage of the personal data;

2. 成员国应要求数据控制者采取适当的技术和组织措施，确保在默认情况下仅处理与特定处理目的相关的必要个人数据。该义务适用于所收集个人数据的数量、处理范围、存储期限及其可访问性。特别地，此类措施应确保在默认情况下，未经个人干预，个人数据不会被无限期地向不特定数量的自然人开放。

第21条

联合控制器

1. 当两个或多个控制者共同确定数据处理的目的和方式时，各成员国应规定其作为共同控制者。各成员国应通过透明方式确定各自在遵守本指令方面的责任，特别是关于数据主体权利的行使及其提供第13条所涉信息的义务，除非且在控制者的责任由其适用的欧盟或成员国法律确定的情况下，可通过双方协议予以明确。该协议应指定数据主体的联系人。成员国可指定联合控制者中哪一方可作为数据主体行使权利的单一联系人。

2. 无论第1款所述安排的具体条款如何，各成员国均可规定数据主体有权依据本指令所采纳的条款，就每个控制者行使自身权利。

第22条

处理机

1. 成员国若需代表控制者进行数据处理，应确保控制者仅使用能提供充分保证的处理方，这些保证需以适当的技术和组织措施实施，从而确保数据处理符合本指令要求并保障数据主体权利。

2. 各成员国应规定，未经控制者事先书面特别授权或一般授权，数据处理者不得聘用其他数据处理者。若获得一般书面授权，则数据处理者须就拟增聘或替换其他数据处理者事宜，向控制者提出变更意向，以便控制者有机会对此类变更提出异议。

3. 成员国应规定，数据处理方须依据欧盟或成员国法律下的合同或其他具有法律约束力的文件进行数据处理。该文件须对控制者具有约束力，明确数据处理的范围与期限、处理目的与性质、个人数据类型及数据主体类别，并规定控制者的权利与义务。该合同或其他法律文件应特别规定：

(a) 仅根据控制器指令执行操作；

(b) 确保授权处理个人数据的人员已承诺遵守保密义务，或依法负有相应的保密责任；

(c) 通过适当方式协助控制者确保遵守数据主体权利的相关规定；

(d) 根据控制者的决定，数据处理服务终止后，应将所有个人数据删除或返还给控制者，并删除现有副本，除非欧盟或成员国法律要求保留个人数据。

(e) makes available to the controller all information necessary to demonstrate compliance with this Article;

(f) complies with the conditions referred to in paragraphs 2 and 3 for engaging another processor.

4. The contract or the other legal act referred to in paragraph 3 shall be in writing, including in an electronic form.

5. If a processor determines, in infringement of this Directive, the purposes and means of processing, that processor shall be considered to be a controller in respect of that processing.

Article 23

Processing under the authority of the controller or processor

Member States shall provide for the processor and any person acting under the authority of the controller or of the processor, who has access to personal data, not to process those data except on instructions from the controller, unless required to do so by Union or Member State law.

Article 24

Records of processing activities

1. Member States shall provide for controllers to maintain a record of all categories of processing activities under their 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 and the data protection officer;

(b) the purposes of the processing;

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

(d) a description of the categories of data subject and of the categories of personal data;

(e) where applicable, the use of profiling;

(f) where applicable, the categories of transfers of personal data to a third country or an international organisation;

(g) an indication of the legal basis for the processing operation, including transfers, for which the personal data are intended;

(h) where possible, the envisaged time limits for erasure of the different categories of personal data;

(i) where possible, a general description of the technical and organisational security measures referred to in Article 29(1).

2. Member States shall provide for each processor to 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, of each controller on behalf of which the processor is acting and, where applicable, 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 where explicitly instructed to do so by the controller, including the identification of that third country or international organisation;

(d) where possible, a general description of the technical and organisational security measures referred to in Article 29(1).

(e) 向控制者提供所有必要信息，以证明符合本条款要求；

(f) 符合第2段和第3段所述的聘用其他处理方的条件。

4. 第3款所述的合同或其他法律行为应以书面形式订立，包括电子形式。

5. 若某处理者判定其处理目的及方式构成对本指令的违反，则该处理者应被视为该处理行为的控制者。

第23条

在控制者或处理者授权下进行处理

各成员国应规定，数据处理者及受控制者或数据处理者授权、可访问个人数据的任何人员，除非欧盟或成员国法律另有要求，否则不得在未经控制者指示的情况下处理这些数据。

第24条

加工活动记录

1. 各成员国应规定控制者对其负责的所有类别处理活动进行记录，该记录应包含以下全部信息：

(a) 控制者的姓名及联系方式，如适用，还包括联合控制者和数据保护官的姓名及联系方式；

(b) 处理的目的；

(c) 已披露或将要披露个人数据的接收方类别，包括第三国或国际组织的接收方；

(d) 数据主体类别及个人数据类别的说明；

(e) 在适用情况下，使用画像技术；

(f) 在适用情况下，个人数据向第三国或国际组织的转移类别；

(g) 个人数据处理操作（包括数据转移）的法律依据说明；

(h) 在可行情况下，拟议的各类个人数据删除时限；

(i) 在可能的情况下，对第29条第1款所述的技术与组织安全措施进行一般性描述。

2. 各成员国应要求每个数据处理者保存由控制者委托开展的所有类型数据处理活动的记录，记录内容包括：

(a) 数据处理者或其代表的每个控制者的名称及联系方式，以及适用情况下数据保护官的姓名及联系方式；

(b) 各控制方委托处理的类别；

(c) 在适用情况下，向第三国或国际组织传输个人数据，前提是控制者已明确指示此类传输，包括明确该第三国或国际组织的身份；

(d) 在可能的情况下，对第29条第1款所述的技术与组织安全措施进行一般性描述。

3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.

The controller and the processor shall make those records available to the supervisory authority on request.

Article 25

Logging

1. Member States shall provide for logs to be kept for at least the following processing operations in automated processing systems: collection, alteration, consultation, disclosure including transfers, combination and erasure. The logs of consultation and disclosure shall make it possible to establish the justification, date and time of such operations and, as far as possible, the identification of the person who consulted or disclosed personal data, and the identity of the recipients of such personal data.

2. The logs shall be used solely for verification of the lawfulness of processing, self-monitoring, ensuring the integrity and security of the personal data, and for criminal proceedings.

3. The controller and the processor shall make the logs available to the supervisory authority on request.

Article 26

Cooperation with the supervisory authority

Member States shall provide for the controller and the processor to cooperate, on request, with the supervisory authority in the performance of its tasks on request.

Article 27

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, Member States shall provide for the controller to carry out, prior to the processing, an assessment of the impact of the envisaged processing operations on the protection of personal data.

2. The assessment referred to in paragraph 1 shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address those risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Directive, taking into account the rights and legitimate interests of the data subjects and other persons concerned.

Article 28

Prior consultation of the supervisory authority

1. Member States shall provide for the controller or processor to consult the supervisory authority prior to processing which will form part of a new filing system to be created, where:

(a) a data protection impact assessment as provided for in Article 27 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk; or

(b) the type of processing, in particular, where using new technologies, mechanisms or procedures, involves a high risk to the rights and freedoms of data subjects.

2. Member States shall provide for the supervisory authority to be consulted 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.

3. Member States shall provide that the supervisory authority may establish a list of the processing operations which are subject to prior consultation pursuant to paragraph 1.

3. 第1段和第2段所述记录应以书面形式保存，包括电子形式。控制者和处理者应根据监管机构要求提供这些记录。

第25条

记录

1. 各成员国应确保自动化处理系统中至少对以下操作记录日志：收集、修改、查阅、披露（包括转移、合并和删除）。查阅与披露的日志应能明确记录操作依据、日期和时间，并尽可能识别查阅或披露个人数据的人员身份，以及该个人数据的接收方身份。

2. 日志仅用于验证处理的合法性、自我监控、确保个人数据的完整性和安全性，以及刑事诉讼。

3. 控制器与处理器应根据监管机构要求提供日志记录。

第26条

与监管机构的合作

各成员国应规定，数据控制者和数据处理者应根据请求与监管机构合作，协助其履行相关职责。

第27条

数据保护影响评估

1. 若某类数据处理（特别是采用新技术的处理）考虑到其性质、范围、背景及目的，可能对自然人的权利和自由构成高风险，成员国应要求数据控制者在处理前，对拟实施的数据处理操作对个人数据保护的影响进行评估。

2. 第1款所述评估应至少包含以下内容：对拟实施的处理操作进行总体描述、对数据主体权利与自由所面临风险的评估、为应对这些风险而拟采取的措施、保障措施、安全措施及机制，以确保个人数据保护并证明符合本指令要求，同时充分考虑数据主体及其他相关方的权利与合法利益。

第28条

事先征询监管机构意见

1. 成员国应规定，当处理行为构成即将建立的新申报系统的一部分时，控制者或处理者须事先征询监管机构意见，具体情形包括：

(a) 根据第27条规定的数据保护影响评估表明，若控制者未采取措施减轻风险，则该处理将导致高风险；或

(b) 特别是涉及使用新技术、新机制或新程序的处理类型，对数据主体的权利和自由构成高风险。

2. 各成员国应规定，在拟由国家议会通过的立法提案或基于该立法提案制定的监管措施（涉及数据处理）的准备过程中，须征询监管机构的意见。

3. 各成员国应规定，监管机构可依据第1款规定，制定需事先协商的处理操作清单。

4. Member States shall provide for the controller to provide the supervisory authority with the data protection impact assessment pursuant to Article 27 and, on request, with any other information to allow the supervisory authority to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.

5. Member States shall, where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 of this Article would infringe the provisions adopted pursuant to this Directive, in particular where the controller has insufficiently identified or mitigated the risk, provide for the supervisory authority to provide, within a period of up to six weeks of receipt of the request for consultation, written advice to the controller and, where applicable, to the processor, and may use any of its powers referred to in Article 47. That period may be extended by a month, 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.

Section 2

Security of personal data

Article 29

Security of processing

1. Member States shall provide for the controller and the processor, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in particular as regards the processing of special categories of personal data referred to in Article 10.

2. In respect of automated processing, each Member State shall provide for the controller or processor, following an evaluation of the risks, to implement measures designed to:

(a) deny unauthorised persons access to processing equipment used for processing ('equipment access control');

(b) prevent the unauthorised reading, copying, modification or removal of data media ('data media control');

(c) prevent the unauthorised input of personal data and the unauthorised inspection, modification or deletion of stored personal data ('storage control');

(d) prevent the use of automated processing systems by unauthorised persons using data communication equipment ('user control');

(e) ensure that persons authorised to use an automated processing system have access only to the personal data covered by their access authorisation ('data access control');

(f) ensure that it is possible to verify and establish the bodies to which personal data have been or may be transmitted or made available using data communication equipment ('communication control');

(g) ensure that it is subsequently possible to verify and establish which personal data have been input into automated processing systems and when and by whom the personal data were input ('input control');

(h) prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media ('transport control');

(i) ensure that installed systems may, in the case of interruption, be restored ('recovery');

(j) ensure that the functions of the system perform, that the appearance of faults in the functions is reported ('reliability') and that stored personal data cannot be corrupted by means of a malfunctioning of the system ('integrity').

4. 各成员国应确保数据控制者根据第27条规定向监管机构提交数据保护影响评估报告，并根据要求提供其他相关信息，以便监管机构评估数据处理的合规性，特别是数据主体个人数据保护风险及相关保障措施。

5. 当监管机构认为本条第1款所述的拟议处理可能违反本指令所采纳的规定时，特别是当控制者未能充分识别或缓解相关风险时，成员国应规定监管机构在收到咨询请求后六周内向控制者提供书面意见，并在适用情况下向处理者提供意见，可行使第47条规定的任何权力。根据拟议处理的复杂程度，该期限可延长一个月。监管机构应在收到咨询请求后一个月内通知控制者及适用情况下处理者有关延期事宜，并说明延迟原因。

第2节

个人数据安全

第29条

处理安全

1. 各成员国应要求控制者和处理者，综合考量技术发展现状、实施成本、数据处理的性质、范围、背景及目的，以及对自然人权利与自由可能产生的风险程度和严重性，采取适当的技术和组织措施，确保安全水平与风险相匹配，尤其针对第10条所述特殊类别的个人数据处理。

2. 在自动化处理方面，各成员国应要求控制者或处理者在评估风险后，采取以下措施：

(a) 禁止未经授权人员接触用于处理的设备（‘设备访问控制’）；

(b) 防止未经授权的数据介质读取、复制、修改或删除（‘数据介质控制’）；

(c) 防止个人数据的未经授权输入，以及存储个人数据的未经授权检查、修改或删除（“存储控制”）；

(d) 防止未经授权人员使用数据通信设备操作自动化处理系统（‘用户控制’）；

(e) 确保有权使用自动化处理系统的人士仅能访问其访问授权所涵盖的个人数据（“数据访问控制”）；

(f) 确保能够验证并建立已传输或可能通过数据通信设备（‘通信控制’）传输或提供个人数据的接收方。

(g) 确保后续能够验证并确认哪些个人数据被输入自动化处理系统，以及这些个人数据的输入时间及输入者（‘输入控制’）；

(h) 防止在个人数据传输或数据介质运输过程中（‘传输控制’）未经授权的个人数据读取、复制、修改或删除；

(i) 确保已安装系统在发生中断时能够恢复（‘恢复’）；

(j) 确保系统功能正常运行，功能故障出现时能及时上报（‘可靠性’），并防止存储的个人数据因系统故障而受损（‘完整性’）。

Article 30

Notification of a personal data breach to the supervisory authority

1. Member States shall, in the case of a personal data breach, provide for the controller to notify without undue delay and, where feasible, not later than 72 hours after having become aware of it, the personal data breach to the supervisory authority, 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. Member States shall provide for the controller to document any personal data breaches referred to in paragraph 1, 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.

6. Member States shall, where the personal data breach involves personal data that have been transmitted by or to the controller of another Member State, provide for the information referred to in paragraph 3 to be communicated to the controller of that Member State without undue delay.

Article 31

Communication of a personal data breach to the data subject

1. Member States shall, where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, provide for the controller to communicate the personal data breach to the data subject without undue delay.

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 shall contain at least the information and measures referred to in points (b), (c) and (d) of Article 30(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 technological 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 a disproportionate effort. In such a case, there shall instead be a public communication or a similar measure whereby the data subjects are informed in an equally effective manner.

第30条

向监管机构通报个人数据泄露事件

1. 成员国在发生个人数据泄露事件时，应确保控制者在发现后不延误通知监管机构，且在可行情况下最迟于72小时内完成通报，除非该泄露事件不太可能对自然人的权利和自由构成风险。若未能在72小时内向监管机构通报，必须附上延迟通报的具体原因。

2. 处理器在发现个人数据泄露后，应立即通知控制者。

3. 第1款所述通知至少应包括：

(a) 描述个人数据泄露的性质，尽可能包括相关数据主体的类别及大致数量，以及相关个人数据记录的类别及大致数量；

(b) 告知数据保护官或其他可获取更多信息的联系人的姓名及联系方式；

(c) 阐述个人数据泄露可能引发的后果；

(d) 描述控制者为应对个人数据泄露所采取或拟采取的措施，包括在适当情况下为减轻其可能产生的不利影响而采取的措施。

4. 若无法同时提供信息，且在无法实现同步提供的情况下，可分阶段提供信息，且不应造成不必要延误。

5. 各成员国应要求数据控制者对第1款所述的任何个人数据泄露事件进行记录，包括相关事实、影响及已采取的补救措施。该记录应使监管机构能够核查本条款的遵守情况。

6. 若个人数据泄露涉及由另一成员国控制者传输或接收的个人数据，各成员国应确保第3款所述信息及时通报该成员国控制者。

第31条

向数据主体通报个人数据泄露事件

1. 若个人数据泄露可能对自然人的权利和自由构成重大风险，成员国应确保控制者及时向数据主体通报该泄露事件。

2. 向本条第1款所述数据主体发出的沟通文件，须以清晰明了的语言说明个人数据泄露的具体情况，并至少包含第30条第3款(b)、(c)、(d)项所列信息及应对措施。

3. 若符合下列任一条件，则无需向第1段所述数据主体进行沟通：

(a) 数据控制者已采取适当的技术与组织防护措施，并将这些措施应用于受影响的个人数据，特别是那些使未经授权人员无法解读个人数据的措施，例如加密技术。

(b) 控制者已采取后续措施，确保第1段所述数据主体权利与自由的高风险不再可能实现；

(c) 这将需要付出不成比例的努力。在此情况下，应采取公开告知或其他类似措施，以同样有效的方式向数据主体进行告知。

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.

5. The communication to the data subject referred to in paragraph 1 of this Article may be delayed, restricted or omitted subject to the conditions and on the grounds referred to in Article 13(3).

Section 3

Data protection officer

Article 32

Designation of the data protection officer

1. Member States shall provide for the controller to designate a data protection officer. Member States may exempt courts and other independent judicial authorities when acting in their judicial capacity from that obligation.

2. The data protection officer shall be designated on the basis of his or her professional qualities and, in particular, his or her expert knowledge of data protection law and practice and ability to fulfil the tasks referred to in Article 34.

3. A single data protection officer may be designated for several competent authorities, taking account of their organisational structure and size.

4. Member States shall provide for the controller to publish the contact details of the data protection officer and communicate them to the supervisory authority.

Article 33

Position of the data protection officer

1. Member States shall provide for the controller to 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.

2. The controller shall support the data protection officer in performing the tasks referred to in Article 34 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.

Article 34

Tasks of the data protection officer

Member States shall provide for the controller to entrust the data protection officer at least with the following tasks:

(a) to inform and advise the controller and the employees who carry out processing of their obligations pursuant to this Directive and to other Union or Member State data protection provisions;

(b) to monitor compliance with this Directive, with other Union or Member State data protection provisions and with the policies of the controller 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 27;

(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 28, and to consult, where appropriate, with regard to any other matter.

4. 若数据控制者尚未向数据主体通报个人数据泄露事件，监管机构在评估该泄露事件可能引发高风险后，可要求其履行告知义务，或认定第3款所述任一条件已满足。

5. 根据第13条第3款所述条件及理由，可延迟、限制或省略向本条第1款所述数据主体的沟通。

第3节

数据保护官

第32条

数据保护官的任命

1. 成员国应规定数据控制者指定数据保护官。成员国可豁免法院及其他独立司法机关在司法职能范围内履行该义务。

2. 数据保护官的任命应基于其专业资质，尤其需具备数据保护法律与实务的专业知识，以及履行第34条所规定职责的能力。

3. 可为多个主管部门指定一名数据保护官，具体人选需根据其组织结构和规模确定。

4. 各成员国应规定数据控制者公布数据保护官的联系方式，并将其通报给监管机构。

第33条

数据保护官的职位

1. 各成员国应确保数据控制者及时妥善地让数据保护官参与所有涉及个人数据保护的事务。

2. 数据控制者应通过提供必要资源、保障个人数据及处理操作的访问权限，并维持其专业知识，协助数据保护官履行第34条规定的职责。

第34条

数据保护官的职责

成员国应确保数据控制者至少可委托数据保护官履行以下职责：

(a) 向数据控制者及履行其根据本指令及其他欧盟或成员国数据保护规定所承担义务的员工提供信息与建议；

(b) 监督本指令的执行情况，确保其与其他欧盟或成员国数据保护法规以及数据控制者关于个人数据保护的政策相一致，具体包括：明确相关责任归属、开展数据处理人员的培训与意识提升活动，以及实施相关审计工作。

(c) 根据第27条规定，就数据保护影响评估提供应要求的建议，并监督其执行情况；

(d) 与监管部门协作；

(e) 作为监管机构在处理相关事务时的联络点，包括第28条所述的事先咨询，并在适当情况下就其他事项进行协商。

CHAPTER V

Transfers of personal data to third countries or international organisations

Article 35

General principles for transfers of personal data

1. Member States shall provide for any transfer by competent authorities of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation including for onward transfers to another third country or international organisation to take place, subject to compliance with the national provisions adopted pursuant to other provisions of this Directive, only where the conditions laid down in this Chapter are met, namely:

(a) the transfer is necessary for the purposes set out in Article 1(1);

(b) the personal data are transferred to a controller in a third country or international organisation that is an authority competent for the purposes referred to in Article 1(1);

(c) where personal data are transmitted or made available from another Member State, that Member State has given its prior authorisation to the transfer in accordance with its national law;

(d) the Commission has adopted an adequacy decision pursuant to Article 36, or, in the absence of such a decision, appropriate safeguards have been provided or exist pursuant to Article 37, or, in the absence of an adequacy decision pursuant to Article 36 and of appropriate safeguards in accordance with Article 37, derogations for specific situations apply pursuant to Article 38; and

(e) in the case of an onward transfer to another third country or international organisation, the competent authority that carried out the original transfer or another competent authority of the same Member State authorises the onward transfer, after taking into due account all relevant factors, including the seriousness of the criminal offence, the purpose for which the personal data was originally transferred and the level of personal data protection in the third country or an international organisation to which personal data are onward transferred.

2. Member States shall provide for transfers without the prior authorisation by another Member State in accordance with point (c) of paragraph 1 to be permitted only if the transfer of the personal data is necessary for the prevention of an immediate and serious threat to public security of a Member State or a third country or to essential interests of a Member State and the prior authorisation cannot be obtained in good time. The authority responsible for giving prior authorisation shall be informed without delay.

3. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons ensured by this Directive is not undermined.

Article 36

Transfers on the basis of an adequacy decision

1. Member States shall provide that 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 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 data protection rules, including adequate enforcement powers, for assisting and advising data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and

第五章

向第三国或国际组织传输个人数据

第35条

个人数据转移的一般原则

1. 成员国应规定，主管当局在向第三国或国际组织转移正在处理或拟处理的个人数据时（包括后续向另一第三国或国际组织的转移），须遵守本指令其他条款所规定的国家规定，且仅在满足本章所列条件时方可进行此类转移。具体条件如下：

(a) 该转让为实现第1条第1款所规定之目的而必要；

(b) 个人数据将被转移至第三国或国际组织的控制者，该控制者是具备第1条第1款所述目的管辖权的机构；

(c) 当个人数据从另一成员国传输或提供时，该成员国已根据其国内法律对该传输行为给予事先授权；

(d) 委员会已根据第36条作出充分性决定，或在未作出此类决定的情况下，已根据第37条提供或存在适当保障措施；若既未根据第36条作出充分性决定，也未根据第37条提供适当保障措施，则应依据第38条对特定情形作出豁免；

(e) 若需将个人数据转交至第三国或国际组织，原数据转移主管部门或同一成员国的其他主管机关须在充分考虑所有相关因素后批准转交，这些因素包括犯罪行为的严重程度、个人数据最初转移的用途，以及接收方所在第三国或国际组织的个人数据保护水平。

2. 成员国应规定，根据第1款(c)项，未经另一成员国事先授权的个人数据转移仅在以下情况下允许：该转移对于防止对成员国或第三国公共安全的直接严重威胁或对成员国基本利益的必要性，且无法及时获得事先授权。负责给予事先授权的主管部门应立即获知此事。

3. 为确保本指令所保障的自然人保护水平不受削弱，本章所有条款均应适用。

第36条

根据充足性决定进行的转移

1. 成员国应规定，若欧盟委员会认定相关第三国、其领土或特定领域，或国际组织能提供充分的保护水平，则可向其传输个人数据。此类传输无需特别授权。

2. 在评估保护水平是否充分时，委员会应特别考虑以下要素：

(a) 法治原则、人权与基本自由的保障、相关立法（包括公共安全、国防、国家安全及刑法领域的通用性与行业性法规）、公共机构获取个人数据的权限及其执行情况、数据保护规则、职业规范与安全措施（含向第三国或国际组织转移个人数据的规则）、该国或国际组织遵循的判例法、数据主体享有的有效可执行权利，以及个人数据被转移时可获得的行政与司法救济机制；

(b) 第三国或国际组织所属国家存在并有效运作的一个或多个独立监督机构，其职责包括：确保并执行数据保护规则（含充分的执法权），协助数据主体行使权利并提供咨询，以及与成员国监督机构开展合作；

(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 a mechanism for 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 58(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.

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 58(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 58(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. Member States shall provide for a decision pursuant to paragraph 5 to be without prejudice to transfers of personal data to the third country, the territory or one or more specified sectors within that third country, or the international organisation in question pursuant to Articles 37 and 38.

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.

Article 37

Transfers subject to appropriate safeguards

1. In the absence of a decision pursuant to Article 36(3), Member States shall provide that a transfer of personal data to a third country or an international organisation may take place where:

(a) appropriate safeguards with regard to the protection of personal data are provided for in a legally binding instrument; or

(b) the controller has assessed all the circumstances surrounding the transfer of personal data and concludes that appropriate safeguards exist with regard to the protection of personal data.

2. The controller shall inform the supervisory authority about categories of transfers under point (b) of paragraph 1.

3. When a transfer is based on point (b) of paragraph 1, such a transfer shall be documented and the documentation shall be made available to the supervisory authority on request, including the date and time of the transfer, information about the receiving competent authority, the justification for the transfer and the personal data transferred.

(c) 第三国或相关国际组织所承担的国际承诺，或因具有法律约束力的公约、文书及其参与多边或区域体系而产生的其他义务，特别是涉及个人数据保护的义务。

3. 委员会在评估保护水平是否充分后，可通过实施性法规决定由第三国、第三国境内的特定区域或一个或多个指定部门，或国际组织确保达到本条第2款所规定的适当保护水平。实施性法规应规定至少每四年进行一次的定期审查机制，该审查需综合考虑第三国或国际组织的所有相关发展动态。实施性法规应明确其地域适用范围和部门适用范围，并在适用情况下指明本条第2款(b)项所提及的监管机构。实施性法规的制定应遵循第58条第2款规定的审查程序。

4. 委员会应持续关注第三国及国际组织可能影响第3款所作决定实施的相关动态。

5. 当委员会根据现有信息（特别是本条第3款所述审查后）发现第三国、第三国领土或其特定部门，或国际组织未能继续提供本条第2款所规定的充分保护时，委员会应通过不溯及既往的实施性法规，在必要范围内废止、修改或暂停本条第3款所述决定。此类实施性法规的制定须遵循第58条第2款规定的审查程序。

基于正当且紧迫的强制性理由，委员会应依照第58条第3款所述程序，立即颁布可立即生效的实施性法规。

6. 委员会应与第三国或国际组织进行磋商，以解决导致根据第5款作出决定的情况。

7. 成员国应确保第5款所作决定不影响根据第37条和第38条向第三国、该第三国的领土或一个或多个特定部门，或相关国际组织传输个人数据。

8. 委员会应在*欧洲联盟官方公报*和其网站上公布一份清单，列出委员会决定对其中的第三国、领土和第三国的特定部门以及国际组织提供或不再提供适当保护的国家。

第37条

受适当保障措施约束的转让

1. 若未依据第36条第3款作出决定，成员国应规定：在以下情况下，可将个人数据转移至第三国或国际组织：

(a) 在具有法律约束力的文件中规定了适当的个人数据保护措施；或

(b) 数据控制者已全面评估个人数据转移相关的所有情况，并确认已采取适当保护措施以确保个人数据安全。

2. 控制方应向监管机构通报第1款(b)项所列的转让类别。

3. 若转让依据第1款(b)项规定，须形成书面记录，并应监管机构要求提供，记录内容包括：转让日期与时间、接收主管机关信息、转让依据及所涉个人数据。

Article 38

Derogations for specific situations

1. In the absence of an adequacy decision pursuant to Article 36, or of appropriate safeguards pursuant to Article 37, Member States shall provide that a transfer or a category of transfers of personal data to a third country or an international organisation may take place only on the condition that the transfer is necessary:

(a) in order to protect the vital interests of the data subject or another person;

(b) to safeguard legitimate interests of the data subject, where the law of the Member State transferring the personal data so provides;

(c) for the prevention of an immediate and serious threat to public security of a Member State or a third country;

(d) in individual cases for the purposes set out in Article 1(1); or

(e) in an individual case for the establishment, exercise or defence of legal claims relating to the purposes set out in Article 1(1).

2. Personal data shall not be transferred if the transferring competent authority determines that fundamental rights and freedoms of the data subject concerned override the public interest in the transfer set out in points (d) and (e) of paragraph 1.

3. Where a transfer is based on paragraph 1, such a transfer shall be documented and the documentation shall be made available to the supervisory authority on request, including the date and time of the transfer, information about the receiving competent authority, the justification for the transfer and the personal data transferred.

Article 39

Transfers of personal data to recipients established in third countries

1. By way of derogation from point (b) of Article 35(1) and without prejudice to any international agreement referred to in paragraph 2 of this Article, Union or Member State law may provide for the competent authorities referred to in point (7)(a) of Article 3, in individual and specific cases, to transfer personal data directly to recipients established in third countries only if the other provisions of this Directive are complied with and all of the following conditions are fulfilled:

(a) the transfer is strictly necessary for the performance of a task of the transferring competent authority as provided for by Union or Member State law for the purposes set out in Article 1(1);

(b) the transferring competent authority determines that no fundamental rights and freedoms of the data subject concerned override the public interest necessitating the transfer in the case at hand;

(c) the transferring competent authority considers that the transfer to an authority that is competent for the purposes referred to in Article 1(1) in the third country is ineffective or inappropriate, in particular because the transfer cannot be achieved in good time;

(d) the authority that is competent for the purposes referred to in Article 1(1) in the third country is informed without undue delay, unless this is ineffective or inappropriate;

(e) the transferring competent authority informs the recipient of the specified purpose or purposes for which the personal data are only to be processed by the latter provided that such processing is necessary.

2. An international agreement referred to in paragraph 1 shall be any bilateral or multilateral international agreement in force between Member States and third countries in the field of judicial cooperation in criminal matters and police cooperation.

3. The transferring competent authority shall inform the supervisory authority about transfers under this Article.

4. Where a transfer is based on paragraph 1, such a transfer shall be documented.

第38条

特定情况下的豁免

1. 若未依据第36条作出充分性决定，或未依据第37条采取适当保障措施，成员国应规定：向第三国或国际组织转移或转移类别的个人数据，仅在确有必要时方可进行。

(a) 为保护数据主体或其他人的合法权益；

(b) 为保护数据主体的合法权益，若个人数据转移成员国的法律规定了相关措施；

(c) 为防范对成员国或第三国公共安全构成的直接且严重威胁；

(d) 在个别情况下，为实现第1条第1款所规定的目的；或

(e) 在个案中，为确立、行使或抗辩与第1条第1款所列目的相关的法律主张。

2. 若主管机关认定相关数据主体的基本权利与自由优先于第1款(d)项和(e)项所列的公共利益，则不得进行个人数据转移。

3. 若转让依据第1款规定，须将相关文件存档，并应监管机构要求提供，文件内容包括：转让日期与时间、接收主管机关信息、转让依据及所涉个人数据。

第39条

向第三国接收方传输个人数据

1. 为对第35条第1款(b)项的例外规定，且不影响本条第2款所提及的任何国际协议，欧盟或成员国法律可规定：在个别具体情况下，第3条第7款(a)项所指的主管当局仅在符合本指令其他规定且满足下列全部条件时，方可将个人数据直接传输至第三国设立的接收方：

(a) 根据欧盟或成员国法律为履行第1条第1款所列目的而规定的任务，转让对转让主管机关的履行具有严格必要性；

(b) 转移主管机关经评估认定，当前案件中相关数据主体的基本权利与自由并不抵触公共利益，故无需进行数据转移。

(c) 若转移主管机关认定，将相关事项移交给第三国第1条第1款所涉事项的主管机关无效或不适当，特别是因无法及时完成转移；

(d) 对于第三国第1条第1款所述目的具有管辖权的主管机关应立即获知，除非该通知无效或不适当；

(e) 数据转移主管机关应告知接收方，个人数据仅在必要时方可为接收方处理，且须明确说明处理目的。

2. 第1款所述国际协议，指成员国与第三国在刑事司法合作及警务合作领域内已生效的双边或多边国际协议。

3. 负责转让的主管部门应当将本条规定的转让事项告知监督管理部门。

4. 若转让依据第1款规定，则此类转让须形成书面文件。

Article 40

International cooperation for the protection of personal data

In relation to third countries and international organisations, the Commission and Member States 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 41

Supervisory authority

1. Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Directive, 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 Directive throughout the Union. For that purpose, the supervisory authorities shall cooperate with each other and with the Commission in accordance with Chapter VII.

3. Member States may provide for a supervisory authority established under Regulation (EU) 2016/679 to be the supervisory authority referred to in this Directive and to assume responsibility for the tasks of the supervisory authority to be established under paragraph 1 of this Article.

4. Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which are to represent those authorities in the Board referred to in Article 51.

Article 42

Independence

1. Each Member State shall provide for each supervisory authority to act with complete independence in performing its tasks and exercising its powers in accordance with this Directive.

2. Member States shall provide for the member or members of their supervisory authorities in the performance of their tasks and exercise of their powers in accordance with this Directive, to remain free from external influence, whether direct or indirect, and that they shall neither seek nor take instructions from anybody.

3. Members of Member States' supervisory authorities 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.

第40条

保护个人数据的国际合作

对于第三国和国际组织，委员会和成员国应采取适当措施：

(a) 建立国际合作机制，以促进个人数据保护立法的有效实施；

(b) 在遵守个人数据保护及其他基本权利与自由的适当保障措施的前提下，通过通知、投诉转介、调查协助及信息交换等方式，为个人数据保护立法的实施提供国际互助。

(c) 在旨在促进个人数据保护立法执行国际合作的讨论和活动中，让相关利益攸关方参与其中；

(d) 促进个人数据保护立法与实践的交流与文件共享，包括与第三国的管辖权冲突问题。

第六章

独立的监督机构

第1节

独立地位

第41条

监督机关

1. 各成员国应设立一个或多个独立的公共监管机构，负责监督本指令的实施，以保障自然人在数据处理方面的基本权利与自由，并促进个人数据在欧盟范围内的自由流动（即‘监管机构’）。

2. 各监管机构应促进本指令在整个欧盟范围内的统一实施。为此，各监管机构应根据第七章的规定，相互协作并配合欧盟委员会。

3. 成员国可规定根据欧盟第2016/679号条例设立的监管机构作为本指令所指监管机构，并负责履行本条第1款规定设立的监管机构的职责。

4. 若某成员国设有多个监管机构，则该成员国应指定代表这些机构在第51条所指理事会中的监管机构。

第42条

独立

1. 各成员国应确保每个监管机构在履行职责和行使权力时完全独立，且符合本指令要求。

2. 各成员国应确保其监管机构成员在履行职责和行使权力时，不受任何直接或间接的外部影响，且不得向任何人寻求或接受指示。

3. 各成员国监管机构成员应避免采取与其职责相冲突的任何行为，且在任职期间不得从事任何不相容的职业，无论是否具有报酬。

4. 各成员国应确保为各监管机构提供必要的人力、技术、资金、办公场所及基础设施，以有效履行其职责并行使权力，包括在董事会框架内开展的相互协助、合作与参与相关事务。

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 43

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 their duties and exercise their 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 44

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;

(b) the qualifications and eligibility conditions required to be appointed as a 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 not less than four years, except for the first appointment after 6 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 the 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 Directive.

5. 各成员国应确保各监管机构自行选择并配备工作人员，且该工作人员须完全服从相关监管机构成员的专属指挥。

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管控，并拥有独立的年度公共预算，该预算可纳入国家或整体预算体系。

第43条

监察机关成员的任职条件

1. 各成员国应通过透明程序为其监督机构的每位成员提供以下安排：

——他们的议会；

——他们的政府；

—国家元首；或

— 一个根据成员国法律授权的独立机构。

2. 每位成员均应具备履行职责和行使权力所需的资质、经验和技能，特别是在个人数据保护领域。

3. 成员的职责在任期届满、辞职或强制退休时终止，具体依照相关成员国的法律规定执行。

4. 只有在成员存在严重不当行为或不再符合履职条件时，方可予以解聘。

第44条

关于设立监督机构的规则

1. 各成员国应通过立法规定以下全部内容：

(a) 各监管机构的设立；

(b) 各监管机构成员的任职资格与准入条件；

(c) 各监管机构成员的任命规则与程序；

(d) 各监管机构成员的任期不得少于四年，但2016年5月6日之后的首次任命除外。若需通过轮换任命程序保障监管机构独立性，则可适当缩短该首次任命的任期。

(e) 各监管机构成员是否具备连任资格，若具备则连任任期为多少；

(f) 各监管机构成员及工作人员的义务适用条件、任职期间及离职后禁止从事的不相容行为、职业及利益，以及离职规则。

2. 各监管机构的成员及工作人员，须依据欧盟或成员国法律，在任职期间及离职后，对其在履职过程中获知的任何机密信息承担职业保密义务。任职期间，该保密义务尤其适用于自然人举报违反本指令的行为。

Section 2

Competence, tasks and powers

Article 45

Competence

1. Each Member State shall provide for each supervisory authority to be competent for the performance of the tasks assigned to, and for the exercise of the powers conferred on, it in accordance with this Directive on the territory of its own Member State.

2. Each Member State shall provide for each supervisory authority not to be competent for the supervision of processing operations of courts when acting in their judicial capacity. Member States may provide for their supervisory authority not to be competent to supervise processing operations of other independent judicial authorities when acting in their judicial capacity.

Article 46

Tasks

1. Each Member State shall provide, on its territory, for each supervisory authority to:

(a) monitor and enforce the application of the provisions adopted pursuant to this Directive and its implementing measures;

(b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing;

(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 Directive;

(e) upon request, provide information to any data subject concerning the exercise of their rights under this Directive and, if appropriate, cooperate with the supervisory authorities in other Member States to that end;

(f) deal with complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 55, 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) check the lawfulness of processing pursuant to Article 17, and inform the data subject within a reasonable period of the outcome of the check pursuant to paragraph 3 of that Article or of the reasons why the check has not been carried out;

(h) cooperate with, including by sharing information, and provide mutual assistance to other supervisory authorities, with a view to ensuring the consistency of application and enforcement of this Directive;

(i) conduct investigations on the application of this Directive, including on the basis of information received from another supervisory authority or other public authority;

(j) monitor relevant developments insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies;

(k) provide advice on the processing operations referred to in Article 28; and

(l) contribute to the activities of the Board.

2. Each supervisory authority shall facilitate the submission of complaints referred to in point (f) of paragraph 1 by measures such as providing a complaint submission form which can also be completed electronically, without excluding other means of communication.

第2节

权限、任务和权力

第45条

能力

1. 各成员国应确保其境内各监管机构具备履行本指令所赋予任务及行使相应权力的能力。

2. 各成员国应规定，其监管机构在行使司法职能时，不得对法院的审理程序行使监督权。成员国亦可规定，其监管机构在行使司法职能时，不得对其他独立司法机关的审理程序行使监督权。

第46条

任务

1. 各成员国应在其境内为每个监管机构提供：

(a) 监督并确保本指令及其实施措施所采纳条款的落实；

(b) 提高公众对数据处理相关风险、规则、保障措施及权利的认知与理解；

(c) 根据成员国法律，就涉及自然人数据处理权利与自由保护的立法及行政措施，向国家议会、政府及其他相关机构提供咨询意见。

(d) 提高控制器和处理器对本指令所规定义务的认知；

(e) 应要求，向任何数据主体提供有关其根据本指令行使权利的信息，并在适当情况下为此目的与其他成员国的监管机构合作；

(f) 处理数据主体或根据第55条由机构、组织或协会提出的投诉，并酌情调查投诉事项，于合理期限内向投诉人通报调查进展及结果，特别是当需进一步调查或与另一监管机构协调时；

(g) 根据第17条核查数据处理的合法性，并在合理期限内向数据主体告知核查结果（依据该条第3款）或未执行核查的原因；

(h) 与其他监管机构开展合作，包括共享信息，并提供相互协助，以确保本指令的适用与执行保持一致；

(i) 对本指令的适用开展调查，包括根据从其他监管机构或其他公共机构获得的信息进行调查；

(j) 监测相关发展动态，特别是信息和通信技术的发展，这些动态对个人数据保护具有影响；

(k) 就第28条所述的加工操作提供咨询意见；

(l) 参与董事会的各项活动。

2. 各监管机构应通过提供可电子填写的投诉提交表等措施，便利提交第1段(f)项所述投诉，同时不排除其他沟通方式。

3. The performance of the tasks of each supervisory authority shall be free of charge for the data subject and for the data protection officer.

4. Where a request is manifestly unfounded or excessive, in particular because it is repetitive, the supervisory authority may charge a reasonable fee based on its administrative costs, or may refuse to act on the request. The supervisory authority shall bear the burden of demonstrating that the request is manifestly unfounded or excessive.

Article 47

Powers

1. Each Member State shall provide by law for each supervisory authority to have effective investigative powers. Those powers shall include at least the power to obtain from the controller and the processor access to all personal data that are being processed and to all information necessary for the performance of its tasks.

2. Each Member State shall provide by law for each supervisory authority to have effective corrective powers such as, for example:

(a) to issue warnings to a controller or processor that intended processing operations are likely to infringe the provisions adopted pursuant to this Directive;

(b) to order the controller or processor to bring processing operations into compliance with the provisions adopted pursuant to this Directive, where appropriate, in a specified manner and within a specified period, in particular by ordering the rectification or erasure of personal data or restriction of processing pursuant to Article 16;

(c) to impose a temporary or definitive limitation, including a ban, on processing.

3. Each Member State shall provide by law for each supervisory authority to have effective advisory powers to advise the controller in accordance with the prior consultation procedure referred to in Article 28 and to issue, on its own initiative or on request, opinions to its national parliament and its government or, in accordance with its national law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data.

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, as set out in Union and Member State law in accordance with the Charter.

5. Each Member State shall provide by law for each supervisory authority to have the power to bring infringements of provisions adopted pursuant to this Directive to the attention of judicial authorities and, where appropriate, to commence or otherwise engage in legal proceedings, in order to enforce the provisions adopted pursuant to this Directive.

Article 48

Reporting of infringements

Member States shall provide for competent authorities to put in place effective mechanisms to encourage confidential reporting of infringements of this Directive.

Article 49

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 penalties imposed. 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, the Commission and the Board.

3. 各监管机构的任务执行应免费提供给数据主体及数据保护官。

4. 若请求明显缺乏依据或过度，特别是重复性请求，监管机构可依据行政成本收取合理费用，或不予受理。监管机构须承担举证责任，证明该请求确属明显缺乏依据或过度。

第47条

幂

1. 各成员国应通过立法确保每个监管机构均具备有效的调查权。此类调查权至少应包括：向数据控制者及处理者获取正在处理的所有个人数据，以及履行职责所需的所有信息。

2. 各成员国应通过立法赋予各监管机构有效的纠正权力，例如：

(a) 向控制器或处理器发出警告，因其拟执行的处理操作可能违反本指令所采纳的规定；

(b) 责令控制者或处理者在适用情况下，以特定方式并在规定期限内，使处理操作符合本指令所采纳的规定，特别是通过根据第16条责令更正或删除个人数据或限制处理；

(c) 对加工活动实施临时或永久性限制，包括禁止。

3. 各成员国应通过立法赋予各监管机构有效咨询权，使其能够依照第28条规定的事先协商程序向数据控制者提供建议，并可主动或应要求就个人数据保护相关事宜向本国议会、政府或其他机构及公众发表意见。

4. 根据本条授予的监督机构行使权力时，须依照《宪章》规定，遵循欧盟及成员国法律确立的适当保障措施，包括有效的司法救济和正当程序。

5. 各成员国应通过立法赋予各监管机构权力，使其有权将违反本指令所采纳条款的行为通报司法机关，并在适当情况下启动或以其他方式开展法律程序，以确保本指令所采纳条款的实施。

第48条

侵权行为的报告

各成员国应授权主管当局建立有效机制，鼓励对本指令的违规行为进行保密举报。

第49条

活动报告

各监管机构须编制年度工作报告，内容应包含已通报的违规类型及处罚措施清单。报告需提交至国家议会、政府及成员国法律规定的其他主管部门，并向公众、欧盟委员会及理事会公开。

CHAPTER VII

Cooperation

Article 50

Mutual assistance

1. Each Member State shall provide for their supervisory authorities to provide each other with relevant information and mutual assistance in order to implement and apply this Directive in a consistent manner, and to 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 consultations, inspections and investigations.

2. Each Member States shall provide for each supervisory authority to 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 Directive 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. 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. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 58(2).

Article 51

Tasks of the Board

1. The Board established by Regulation (EU) 2016/679 shall perform all of the following tasks in relation to processing within the scope of this Directive:

(a) advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Directive;

(b) 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 Directive and issue guidelines, recommendations and best practices in order to encourage consistent application of this Directive;

(c) draw up guidelines for supervisory authorities concerning the application of measures referred to in Article 47(1) and (3);

(d) issue guidelines, recommendations and best practices in accordance with point (b) of this subparagraph for establishing personal data breaches and determining the undue delay referred to in Article 30(1) and (2) and for the particular circumstances in which a controller or a processor is required to notify the personal data breach;

第七章

合作

第50条

互助

1. 各成员国应确保其监管机构相互提供相关信息并开展互助，以统一方式实施和适用本指令，并建立有效合作机制。互助应特别涵盖信息请求及监管措施，例如开展磋商、检查和调查的请求。

2. 各成员国应确保各监管机构在收到其他监管机构的请求后，须在一个月内采取一切必要措施予以回应，且不得延误。此类措施尤其包括传递调查过程中产生的相关信息。

3. 援助请求应包含所有必要信息，包括请求的目的和理由。所交换的信息仅用于其请求的用途。

4. 请求的监管机构不得拒绝遵守该请求，除非：

(a) 对于所请求的事项或要求执行的措施，其不具备相应权限；或

(b) 若接受请求的监管机构未遵守该指令或欧盟/成员国法律，则将构成对该指令或相关法律的违反。

5. 被请求监管机构应向请求监管机构通报处理结果，或视情况通报为响应请求所采取措施的进展情况。若拒绝遵守第4款规定的要求，被请求监管机构须说明拒绝理由。

6. 被请求的监管机构通常应以电子方式提供其他监管机构所要求的信息，且需采用标准化格式。

7. 被请求的监管机构不得就其根据互助请求采取的任何行动收取费用。在特殊情况下，监管机构可就因提供互助而产生的特定支出相互赔偿事宜达成协议。

8. 委员会可通过实施性法规，具体规定本条所述的相互协助格式与程序，以及监管机构之间、监管机构与董事会之间通过电子方式交换信息的安排。此类实施性法规的制定须遵循第58(2)条规定的审查程序。

第51条

理事会的任务

1. 根据欧盟第2016/679号条例设立的委员会，应就本指令范围内的处理工作履行以下全部职责：

(a) 就欧盟个人数据保护相关事宜向委员会提出建议，包括对本指令任何拟议修订的建议；

(b) 应其成员之一或委员会的请求，主动审查与本指令实施相关的任何问题，并发布指导方针、建议及最佳实践，以促进本指令的统一实施；

(c) 制定监管机构关于第47条第1款和第3款所涉措施适用的指导方针；

(d) 根据本款(b)项规定，制定相关指南、建议及最佳实践，用于界定个人数据泄露情形、判定第30条第1款与第2款所述的不当延迟，以及明确数据控制者或处理者需通报个人数据泄露的具体情形。

(e) issue guidelines, recommendations and best practices in accordance with point (b) of this subparagraph as to the circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons as referred to in Article 31(1);

(f) review the practical application of the guidelines, recommendations and best practices referred to in points (b) and (c);

(g) provide the Commission with an opinion for the assessment of the adequacy of the level of protection in a third country, a territory or one or more specified sectors within a third country, or an international organisation, including for the assessment whether such a third country, territory, specified sector, or international organisation no longer ensures an adequate level of protection;

(h) promote the cooperation and the effective bilateral and multilateral exchange of information and best practices between the supervisory authorities;

(i) 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;

(j) promote the exchange of knowledge and documentation on data protection law and practice with data protection supervisory authorities worldwide.

With regard to point (g) of the first subparagraph, the Commission shall provide the Board with all necessary documentation, including correspondence with the government of the third country, with the territory or specified sector within that third country, or with the international organisation.

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 58(1) and make them public.

4. The Commission shall inform the Board of the action it has taken following opinions, guidelines, recommendations and best practices issued by the Board.

CHAPTER VIII

Remedies, liability and penalties

Article 52

Right to lodge a complaint with a supervisory authority

1. Without prejudice to any other administrative or judicial remedy, Member States shall provide for every data subject to have the right to lodge a complaint with a single supervisory authority, if the data subject considers that the processing of personal data relating to him or her infringes provisions adopted pursuant to this Directive.

2. Member States shall provide for the supervisory authority with which the complaint has been lodged to transmit it to the competent supervisory authority, without undue delay if the complaint is not lodged with the supervisory authority that is competent pursuant to Article 45(1). The data subject shall be informed about the transmission.

3. Member States shall provide for the supervisory authority with which the complaint has been lodged to provide further assistance on request of the data subject.

4. The data subject shall be informed by the competent supervisory authority of the progress and the outcome of the complaint, including of the possibility of a judicial remedy pursuant to Article 53.

Article 53

Right to an effective judicial remedy against a supervisory authority

1. Without prejudice to any other administrative or non-judicial remedy, Member States shall provide for the right of a natural or legal person to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.

(e) 根据本款(b)项规定，就个人数据泄露可能对《欧盟通用数据保护条例》第31条第1款所述自然人权利与自由构成高风险的情形，制定相关指南、建议及最佳实践。

(f) 审查(b)和(c)中提到的指南、建议和最佳实践的实际应用；

(g) 向委员会提交意见，用于评估第三国、其领土或特定部门，以及国际组织的保护水平是否达标，包括判定这些实体是否已无法提供充分保护。

(h) 促进监管机构间的合作，以及双边和多边信息与最佳实践的有效交流；

(i) 推动共同培训计划的实施，并促进监管机构之间、适当时与第三国监管机构或国际组织之间的人员交流；

(j) 促进全球数据保护监管机构就数据保护法律与实践开展知识与文件交流。

关于第一款(g)项，委员会须向董事会提交全部必要文件，包括与第三国政府、该国境内特定区域或部门，以及国际组织的往来函件。

2. 当委员会要求董事会提供意见时，可视事项紧急程度设定时限。

3. 董事会应将其意见、指南、建议及最佳实践提交至委员会及第58(1)条所指委员会，并予以公开。

4. 委员会应向董事会通报其在收到董事会意见、指南、建议及最佳实践后所采取的行动。

第八章

补救措施、责任和处罚

第52条

向监督机关提出申诉的权利

1. 在不影响其他行政或司法救济措施的前提下，各成员国应确保每位数据主体有权向单一监管机构提出投诉，若该数据主体认为其个人数据处理行为违反了本指令所规定的条款。

2. 各成员国应确保投诉提交的监管机构能够及时将投诉转交至主管监管机构，若投诉未按第45条第1款规定提交至主管监管机构，则不得无故拖延。数据主体应获知转交情况。

3. 各成员国应确保投诉所涉监管机构在数据主体提出请求时提供进一步协助。

4. 主管监管机构应向数据主体告知投诉的进展及结果，包括根据第53条可能采取的司法救济途径。

第53条

对监察机关的司法救济权

1. 在不影响其他行政或非司法救济措施的前提下，各成员国应保障自然人或法人在针对其作出的具有法律约束力的监管机构决定时，享有获得有效司法救济的权利。

2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to an effective judicial remedy where the supervisory authority which is competent pursuant to Article 45(1) does not handle a complaint or does not inform the data subject within three months of the progress or outcome of the complaint lodged pursuant to Article 52.

3. Member States shall provide for proceedings against a supervisory authority to be brought before the courts of the Member State where the supervisory authority is established.

Article 54

Right to an effective judicial remedy against a controller or processor

Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 52, Member States shall provide for the right of a data subject to an effective judicial remedy where he or she considers that his or her rights laid down in provisions adopted pursuant to this Directive have been infringed as a result of the processing of his or her personal data in non-compliance with those provisions.

Article 55

Representation of data subjects

Member States shall, in accordance with Member State procedural law, provide for the data subject to have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with Member State law, has statutory objectives which are in the public interest and is active in the field of protection of data subject's rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf and to exercise the rights referred to in Articles 52, 53 and 54 on his or her behalf.

Article 56

Right to compensation

Member States shall provide for any person who has suffered material or non-material damage as a result of an unlawful processing operation or of any act infringing national provisions adopted pursuant to this Directive to have the right to receive compensation for the damage suffered from the controller or any other authority competent under Member State law.

Article 57

Penalties

Member States shall lay down the rules on penalties applicable to infringements of the provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive.

CHAPTER IX

Implementing acts

Article 58

Committee procedure

1. The Commission shall be assisted by the committee established by Article 93 of Regulation (EU) 2016/679. 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.

2. 在不影响其他行政或非司法救济措施的前提下，若根据第45(1)条有权的监管机构未处理投诉，或未在三个月内告知数据主体第52条所提投诉的处理进展或结果，数据主体有权获得有效的司法救济。

3. 成员国应规定，针对监管机构的诉讼程序应提交至该监管机构设立地的成员国法院。

第54条

对控制者或处理者寻求有效司法救济的权利

在不影响任何现有行政或非司法救济措施的前提下（包括根据第52条向监管机构提出投诉的权利），各成员国应保障数据主体在认为其根据本指令所采纳条款享有的权利因个人数据处理未遵守该条款而受到侵害时，获得有效司法救济的权利。

第55条

数据主体的代表

各成员国应依据本国程序法，保障数据主体有权委托符合下列条件的非营利机构、组织或协会：该机构须依法成立，具有符合公共利益的法定宗旨，并在保护数据主体个人数据权利与自由领域积极开展工作，代表数据主体提出投诉并行使《通用数据保护条例》第52、53及54条所规定的相关权利。

第56条

获得赔偿的权利

各成员国应保障因非法数据处理操作或违反本指令所制定国家法规的行为而遭受实质或非实质损害的个人，有权向控制者或成员国法律授权的其他主管机关获得损害赔偿。

第57条

处罚

各成员国应制定针对违反本指令所采纳条款的处罚规则，并采取一切必要措施确保其实施。所规定的处罚应具有效力、适度性及威慑力。

第九章

执行行为

第58条

委员会程序

1. 委员会应由《欧盟条例》（EU）2016/679第93条设立的委员会提供协助。该委员会应为《欧盟条例》（EU）No 182/2011所定义的委员会。

2. 如本段所述，应适用第182/2011号欧盟法规第5条。

3. 凡涉及本段内容时，应适用《欧盟第182/2011号条例》第8条及其第5条的规定。

CHAPTER X

Final provisions

Article 59

Repeal of Framework Decision 2008/977/JHA

1. Framework Decision 2008/977/JHA is repealed with effect from 6 May 2018.

2. References to the repealed Decision referred to in paragraph 1 shall be construed as references to this Directive.

Article 60

Union legal acts already in force

The specific provisions for the protection of personal data in Union legal acts that entered into force on or before 6 May 2016 in the field of judicial cooperation in criminal matters and police cooperation, which regulate processing between Member States and the access of designated authorities of Member States to information systems established pursuant to the Treaties within the scope of this Directive, shall remain unaffected.

Article 61

Relationship with previously concluded international agreements in the field of judicial cooperation in criminal matters and police cooperation

International agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to 6 May 2016 and which comply with Union law as applicable prior to that date shall remain in force until amended, replaced or revoked.

Article 62

Commission reports

1. By 6 May 2022, and every four years thereafter, the Commission shall submit a report on the evaluation and review of this Directive 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 Chapter V on the transfer of personal data to third countries or international organisations with particular regard to decisions adopted pursuant to Article 36(3) and Article 39.

3. For the purposes of paragraphs 1 and 2, 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 with a view to amending this Directive, in particular taking account of developments in information technology and in the light of the state of progress in the information society.

6. By 6 May 2019, the Commission shall review other legal acts adopted by the Union which regulate processing by the competent authorities for the purposes set out in Article 1(1) including those referred to in Article 60, in order to assess the need to align them with this Directive and to make, where appropriate, the necessary proposals to amend those acts to ensure a consistent approach to the protection of personal data within the scope of this Directive.

第十章

最后条款

第59条

废除框架决定2008/977/ JHA

1. 2018年5月6日起废止框架决定2008/977/ JHA 。

2. 第1段中提及的已废止决定应解释为对本指令的引用。

第60条

已生效的工会法律

2016年5月6日或之前生效的欧盟法律文件中关于刑事司法合作与警务合作领域个人数据保护的具体规定，若涉及成员国间数据处理及成员国指定机构访问本指令范围内条约所设信息系统的内容，其效力不受影响。

第61条

与刑事司法合作及警务合作领域既往缔结的国际协定的关系

成员国在2016年5月6日之前缔结的涉及向第三国或国际组织传输个人数据的国际协议，若在该日期前适用的欧盟法律要求其符合规定，则该协议应继续有效，直至被修订、取代或废止。

第62条

委员会报告

1. 委员会应于2022年5月6日及此后每四年向欧洲议会和理事会提交关于本指令评估与审查的报告。报告应予以公开。

2. 在第1段所述的评估与审查过程中，委员会应重点审查第五章关于向第三国或国际组织传输个人数据的规定的适用与实施情况，尤其要特别关注根据第36(3)条和第39条作出的决定。

3. 为实施第1款和第2款之目的，委员会可向成员国及监管机构索取相关信息。

4. 在开展第1段和第2段所述的评估与审查工作时，委员会应充分考虑欧洲议会、理事会及其他相关机构或来源的立场与结论。

5. 委员会应视情况提出适当建议，以修订本指令，尤其需结合信息技术发展动态，并参考信息社会的现状。

6. 欧盟委员会应于2019年5月6日前，对联盟为实现第1条第1款规定目的而制定的其他法律文件（包括第60条提及的文件）进行审查，评估其与本指令的协调需求，并在必要时提出修订建议，以确保在本指令适用范围内对个人数据保护采取统一标准。

Article 63

Transposition

1. Member States shall adopt and publish, by 6 May 2018, the laws, regulations and administrative provisions necessary to comply with this Directive. They shall forthwith notify to the Commission the text of those provisions. They shall apply those provisions from 6 May 2018.

When Member States adopt those provisions, they shall contain a reference to this Directive or shall be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.

2. By way of derogation from paragraph 1, a Member State may provide, exceptionally, where it involves disproportionate effort, for automated processing systems set up before 6 May 2016 to be brought into conformity with Article 25(1) by 6 May 2023.

3. By way of derogation from paragraphs 1 and 2 of this Article, a Member State may, in exceptional circumstances, bring an automated processing system as referred to in paragraph 2 of this Article into conformity with Article 25(1) within a specified period after the period referred to in paragraph 2 of this Article, if it would otherwise cause serious difficulties for the operation of that particular automated processing system. The Member State concerned shall notify the Commission of the grounds for those serious difficulties and the grounds for the specified period within which it shall bring that particular automated processing system into conformity with Article 25(1). The specified period shall in any event not be later than 6 May 2026.

4. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

Article 64

Entry into force

This Directive shall enter into force on the day following that of its publication in the *Official Journal of the European Union*.

Article 65

Addressees

This Directive is addressed to the 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

第63条

转位

1. 各成员国应于2018年5月6日前通过并公布为遵守本指令所必需的法律、法规及行政规定，同时应立即将这些规定的文本通知欧盟委员会，并自2018年5月6日起实施。

各成员国在通过这些条款时，应包含对本指令的引用，或在正式公布时附有此类引用。成员国应确定如何进行此类引用。

2. 作为对第1款的例外规定，成员国可酌情规定：若涉及不成比例的投入，2016年5月6日前建立的自动化处理系统，可于2023年5月6日前完成第25条第1款的合规。

3. 作为对本条第1款和第2款的例外规定，成员国在特殊情况下可采取以下措施：若自动处理系统若不遵守本条第2款规定将导致严重运行困难，则可在该系统运行困难发生后的特定期限内，促使该系统符合第25条第1款要求。相关成员国须向欧盟委员会提交两份文件：一是导致严重运行困难的具体原因说明，二是设定该系统合规期限的依据。特别需要强调的是，该合规期限最迟不得超过2026年5月6日。

4. 各成员国应向委员会通报其在本指令所涵盖领域内通过的国内法主要条款文本。

第64条

生效

本指令在*欧盟官方公报*发布后次日生效。

第65条

收件人

本指令适用于各成员国。

2016年4月27日于布鲁塞尔完成。

致欧洲议会主席的信	*对理事会主席而言*
M. SCHULZ	J. A. 赫尼斯-普拉沙尔特