JCLU
公益社団法人 自由人権協会
Since1947

犯罪の予防、捜査、取調べ検知若しくは起訴、又は刑罰の執行を目的として、所轄官庁により実施される個人データの処理に関する自然人の保護、並びに当該データの自由な移転に関する、EU 理事会枠組み決定 2008/977/JHA を廃止する 2016 年 4 月 27 日 欧州議会及び EU 理事会指令 2016/680

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

欧州議会及び EU 理事会は、
EU の機能に関する条約、とりわけ同条約 16 条 2 項を考慮し、
欧州委員会からの提案を考慮し、
各国の議会に立法案を送付した後、
地域委員会の意見を考慮し、
通常の立法手続に従い、

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) 個人データの処理における自然人の保護は、基本的な権利である。EU 基本権憲章（「憲章」）8 条 1 項及び EU の機能に関する条約（TFEU／EU 機能条約）16 条 1 項は、何人もその個人データの保護を受ける権利を有すると定めている。

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) 個人データの処理における自然人の保護に関する原則及びルールは、国籍又は居住地にかかわらず、基本権及び自由、とりわけ個人データの保護を受ける権利を尊重するものでなければならない。本指令は、自由、安全及び正義の領域の実現に資することを企図している。

[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.

2019.11 公開版

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) テクノロジーの急速な発展及びグローバリゼーションは、個人データの保護に新しい課題をもたらした。個人データの収集及び共有の規模は、著しく拡大している。テクノロジーによって、犯罪の予防、捜査、取調べ検知若しくは起訴、又は刑罰の執行などの活動のために、かつてなかった規模で個人データを処理することが可能となっている。

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) EU 内における公共の安全に対する脅威への安全措置及び予防活動を含む、犯罪の予防、捜査、取調べ検知若しくは起訴、又は刑罰の執行の目的のために、所轄官庁間で行われる個人データの自由な流通、及びかかる個人情報データの第三国及び国際機関への移転は、個人情報データを高度な水準で保護しつつ、促進されるべきである。これらの状況の結果、EU において、強力な執行によって裏付けられた、個人情報データの保護のためのより強力で一貫性のある枠組みを設置することが必要となっている。

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) 欧州議会及び理事会の 95/46/EC 指令は、公的及び民間のセクターの両方について、加盟国におけるすべての個人データの処理に適用される。しかし、同指令は、EU 法 EC 法の範囲外の活動、すなわち刑事事件における司法共助及び警察協力の分野の活動における個人データの処理には適用されない。

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.

---

[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).

(6) EU 理事会枠組み決定 2008/977/JHA は、刑事事件における司法共助及び警察協力の分野に適用される。枠組み決定の適用範囲は、加盟国間で送信され又は利用可能とされた個人データの処理に限定されている。

Council Framework Decision 2008/977/JHA[4] 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) 自然人の個人データが一貫して高度の水準の保護を受けることを確実にすること及び加盟国の所轄官庁の間の個人データのやりとりを支援することは、刑事事件における司法共助及び警察協力が効果的になされるためにきわめて重要なことである。このため、公共の安全に対する脅威への安全措置及び予防活動を含む、犯罪の予防、捜査、検知若しくは起訴、又は刑罰の執行を目的として、所轄官庁により実施される個人データの処理における自然人の権利及び自由の保護の水準は、すべての加盟国において同等であるべきである。EU 全域を通じて個人データを効果的に保護するためには、データ主体の権利の強化及び個人データを処理する者の義務の強化に加え、加盟国において個人データの保護のためのルールを監視しその遵守を確実にするための同等の権限を必要とする。

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) EU 機能条約 16 条 2 項は、欧州議会及び EU 理事会が、個人データの処理における自然人の保護に関するルール及び個人データの自由な移転に関するルールを制定すべきことを定めている。

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.

[4] 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).

(9) これに基づき、欧州議会及びEU理事会の規則2016/679（EU一般データ保護規則／GDPR）は、個人データの処理に関して自然人を保護し、EU 内における個人データの自由な移転を確実にするための一般的なルールを定めている。

On that basis, Regulation (EU) 2016/679 of the European Parliament and of the Council[5] 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) リスボン条約を策定した政府間会議の最終決議に付属する、刑事事件における司法共助及び警察協力の分野における個人データの保護に関する宣言第 21 号において、同会議は、刑事事件における司法共助及び警察協力の分野の特別な性質に照らし、かかる分野における個人データの保護及び個人データの自由な移転について、EU 機能条約 16 条に基づく具体的なルールが必要となりうることを認めた。

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) したがって、これらの分野については、公共の安全に対する脅威への安全措置及び予防活動を含む、犯罪の予防、捜査、検知若しくは起訴、又は刑罰の執行の目的のために所轄官庁が行う個人データの処理における自然人の保護に関する具体的なルールを定める指令において、これらの活動の具体的な性質に配慮した上で、取り扱うことが適切である。かかる所轄官庁とは、司法機関、警察又は他の法執行機関などの公的機関のみならず、加盟国法に基づき、本指令の目的のために公的権限及び公権力を行使できるものとされたその他のいかなる団体又は主体をも含む。かかる団体又は主体が、本指令の目的以外の目的のために個人データを処理する場合は、GDPR が適用される。すなわち、GDPR は、ある団体又は主体が他の目的のために個人データを収集し、さらに当該団体又は主体が負っている法的義務を履行するために当該個人データを処理する場合に適用される。例えば、金融機関は、捜査又は犯罪の訴追の目的のため、自らが処理する一定の個人データを保持しており、加盟国法に従い、また具体的な事件において所轄する国家官庁に対してのみ、当該個人データを提供する。本指令の範囲内でかかる官庁に代わって個人データを処理する団体又は主体は、契約等の法的行為、及び本指令に基づき処理者に適用される規定に拘束されるべきである。他方、当該処理者が本指令の範囲外で行う個人データの処理には、引き続き GDPR が適用される。

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

[5] 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).

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) 警察又は他の法執行機関の活動は、ある事象が犯罪であるかどうかの事前の知識なくなされる警察活動を含め、犯罪の予防、捜査、検知又は起訴に主として焦点を当てて行われる。かかる活動は、デモや大規模なスポーツイベント及び暴動における警察活動のように、強制的な措置を取ることによる公権力の行使を含むことがある。かかる活動はまた、犯罪につながりうるような、公共の安全及び法によって守られた社会の基本的な価値に対する脅威への安全措置及び予防活動が必要な場面において、警察又は他の法執行機関に課された職務として、法と秩序を維持することを含む。加盟国は、所轄官庁に対し、公共の安全に対する脅威への安全措置及び予防活動を含む、犯罪の予防、捜査、検知若しくは起訴の目的でなされるものではないその他の職務を行わせることがあり、そのような他の目的のためになされる個人データの処理は、EU 法の範囲内にあるかぎり、GDPR の適用を受ける。

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 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) 本指令における犯罪とは、EU 司法裁判所（「司法裁判所」）の解釈する EU 法上の独自の概念を意味する。

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) 本指令は、EU 法の範囲外の活動における個人データの処理には適用されるべきではないため、国家の安全に関する活動、国家の安全上の問題に取り組む機関又は部門の活動、及び EU 条約（TEU）第５編第２章の範囲内の活動において加盟国が行う個人データの処理は、本指令が適用される活動と解すべきではない。

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) EU 全体にわたり同水準の、法的に行使可能な権利による自然人の保護を確保するため、及び所轄官庁間の個人データのやりとりを妨げるような不統一を防ぐため、本指令は、公共の安全に対する脅威への安全措置及び予防活動を含む、犯罪の予防、捜査、検知若しくは起訴、又は刑罰の執行の目的のために処理される個人データの保護及び自由な移転のために、統一的なルールを定めるべきである。加盟国の法を互いに近づけることにより、加盟国が与えている個人データの保護が減じられることとなるべきではなく、むしろ、EU 内において高水準の保護を確保することが目指されるべきである。加盟国は、所轄官庁による個人データの処理におけるデータ主体の権利及び自由の保護のため、本指令に定めるものよりも高水準の安全措置を定めることを妨げられるべきではない。

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) 本指令は、公文書の公開の原則に影響を与えない。GDPR においては、公文書の公開と個人データの保護の権利との調整を図るため、公的機関又は公的若しくは私的な団体が、公益目的で遂行した職務のために保有する公文書中の個人データは、EU 法又は当該機関又は団体に適用される加盟国法に従って、当該機関又は団体により開示されることができるとされている。

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) 本指令の保護は、その国籍又は居住地にかかわらず、個人データの処理について自然人に適用されるべきである。

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) 潜脱の深刻なリスクを防ぐため、自然人の保護は、技術的に中立的であるべきであり、使用される技術に依拠するものであってはならない。自然人の保護は、個人データがファイリングシステムに含まれ又は含まれることが意図されている場合は、個人データの自動処理とともに、自動処理でない処理に適用されるべきである。特定の基準に基づいて構成されていないファイル又はファイル群及びそのカバーページには、本指令は適用されるべきではない。

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) 欧州議会及び理事会の規則(EC) No 45/2001（行政機関個人データ保護規則）は、EU の組織、団体、オフィス又は機関による個人データの処理に適用される。かかる個人データの処理に適用される行政機関個人データ保護規則及びその他の EU の法的行為は、GDPR の定める原則及びルールに適合するように修正されるべきである。

Regulation (EC) No 45/2001 of the European Parliament and of the Council[6] 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) 本指令は、加盟国が裁判所及びその他の司法機関による個人データの処理、とりわけ司法判断又は刑事手続に関する記録に含まれる個人データに関して、刑事手続に関する国内のルールにおいて、処理の操作及び処理手続を具体的に定めることを妨げるものではない。

[6] 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).

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.

(21) データ保護の原則は、識別子又は識別できる自然人に関するあらゆる情報に適用されなければならない。自然人が識別できるか否かを決定するにあたっては、直接的又は間接的に自然人を識別するために管理者その他の者により行われる選別のように、合理的に利用されうる全ての手段が考慮されるべきである。手段が自然人を識別するために利用されそうか否かを検証するにあたっては、処理を行う時に利用できる技術及び技術の発展を考慮したうえで、識別に要する費用や所要時間のようなすべての客観的要素を斟酌しなければならない。それゆえ、データ保護の原則は、匿名の情報、すなわち、識別された若しくは識別できる自然人に関連しない情報又はデータ主体がもはや識別されなくなるような方法で匿名化された個人データには適用されない。

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) 税務機関若しくは税関、財務調査機関、独立行政機関、証券市場の規制や監督に責任を持つ金融市場に関する機関のように、公的機関が、その公的な任務を履行するために法的義務に基づいて個人データの開示を受けた場合であって、EU 又は加盟国の法律にしたがって、一般の利益のために特定の照会を実施するために必要なものとして個人データを受領した場合、受領者とみなされてはならない。公的機関による開示要求は、常に、書面により理由が付され不定期でファイリンシステム全体にかかわるもの又はファイリングシステムの相互接続に結びつくものであってはならない。それらの公的機関による個人データの処理は、処理の目的に従って適用されるデータ保護ルールを遵守したものでなければならない。

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) 遺伝データは、生理学又は特定の自然人の健康に関する固有の情報をもたらし、問題となる自然人の生物学的サンプルの分析、特に染色体、デオキシリボ核酸（DNA）又はリボ核酸（RNA）分析又は同等の情報の取得を可能とする他の要素の分析から得られる生来の又は獲得された自然人の遺伝特性に関する個人データを意味するものと定義されなければならない。遺伝情報の複雑性及び繊細性を踏まえると、管理者による誤用や様々な目的への再利用の多大なリスクがある。原則として、遺伝特性に基づく差別は禁止される。

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) 健康に関する個人データは、データ主体の過去、現在若しくは将来の肉体的若しくは精神的健康状態に関する情報を明らかにするデータ主体の健康状態に関する全てのデータを含むものでなければならない。これは、欧州議会及び理事会の 2011/24/EU ディレクティブが言及する、健康管理サービスへの登録又は同サービスのその自然人への提供の過程で収集される自然人に関する以下の情報を含まなければならない：健康目的のために自然人を一意的に識別する目的で特別に割り当てられた番号、シンボル、項目；遺伝データ及び生体サンプルからを含む身体部分又は身体の物質の検査又は試験から引き出せる情報；たとえば、医師その他の健康関係の専門家、病院、医療機器若しくは体外臨床検査システムのように情報の出所には関わらない、たとえばデータ主体の病気、身体障害、病気のリスク、病歴、臨床治療又は生理学的若しくは生物医学的状態に関する情報。

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[7] 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

[7] 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).

hospital, a medical device or an in vitro diagnostic test.

(25) すべての加盟国は、国際犯罪警察組織（インターポール）と関連がある。任務を遂行するために、インターポールは、国際犯罪を防止し国際犯罪と戦うために所管の機関を補助する目的で個人データを受領し、保存し、流通させる。それゆえ、個人データの自動処理に関する基本的権利及び自由の尊重を確保しつつ、個人データの効率的な交換を促進することによって、EU とインターポールとの協力を強化することは適切である。個人データが、EU からインターポールへ、EU からインターポールに人員を派遣している国々へ転送される場合、本指令、殊に国際移転に関する条項が適用される。本指令は、理事会の共通ポジション 2005/69/JHA[8]及び理事会決定 2007/533/JHA[9]が規定する特定の判断に影響するものではない。

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) 全ての個人データの処理は、合法的で公正かつ関連する自然人との関係で透明でなければならず、法定する特定の目的のためにのみ処理されなければならない。このことは、法執行機関が、秘密捜査やビデオ監視のような活動を実行することを直ちに妨げるものではない。そのような活動は、法律で規定され、関係する自然人の正当な利益に十分な考慮を払うもので民主主義社会における必要で比例的な方法である限り、公共の安全に対する脅威への安全対策及び予防を含む犯罪行為の予防、捜査、検知若しくは公訴又は刑罰の執行目的で行うことができる。データ保護原則である公正な処理は、憲章の 47 条及び人権と基本的自由の保護のための欧州条約（ECHR）6 条が定義する公正な裁判を受ける権利とは異なった概念である。自然人は、同人の個人データ処理に関連するリスク、ルール、安全措置及び権利並びに処理に関連して自己の権利をどのように行使するかを知らされるべきである。殊に、個人データを処理する特定の目的は、明確かつ合法的で、個人データの収集がなされる時点で決まっていなければならない。個人データは、処理される目的のために適切で関連していなければならない。殊に、収集される個人データは、それが処理される目的のために過度であってはならず、必要以上の長い期間保有されてはならない。個人データは、他の手段では処理の目的が合理的に達成できない場合にのみ処理されるべきである。必要以上に長い期間データが保有されないよう、消去又は期間の見直しのための期限が管理者によって設定されるべきである。加盟国は、公共の利益のため、科学的、統計的又は歴史的利用のためのアーカイブを目的とする個人デ

[8] Council Common Position 2005/69/JHA of 24 January 2005 on exchanging certain data with Interpol (OJ L 27, 29.1.2005, p. 61).

[9] 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).

ータの長期の保存の適切な安全措置を規定すべきである。

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 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) 犯罪行為の予防、捜査、公訴のため、管轄を有する機関は、特定の犯罪行為の予防、捜査、権利又は公訴を事情として収集した個人データを、犯罪行為に対する理解の発展及び検知された異なる犯罪行為同士を結びつけることを目的として、その事情を超えて処理する必要がある。

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) 処理に関連するセキュリティを維持するため及び本指令違反の処理を避けるため、個人データ及び処理に用いられる機器への権限のないアクセス又は利用の回避を含めて、個人データは、適切なレベルのセキュリティ及び秘密保持が保たれる方法で処理されなければならず、さらに、利用できる先端技術、リスクとの関係での実施費用及び保護する個人データの性質を考慮した方法で処理されなければならない。

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) 個人データは、本指令の射程内で特定の明示的かつ合法的な目的で収集されなければならならず、公共の安全に対する脅威への安全措置及び予防を含む犯罪行為の予防、捜査、検知若しくは公訴又は刑罰の執行目的と相容れない目的のために処理されてはならない。当初収集された目的以外の目的で、本指令の射程内にある目的のために、同一又は異なる管理者によって個人データが処理される場合、そのような処理は、適用される法律の条項に従って権限が与えられており、目的のために必要かつ比例的であることを条件に許容される。

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) データの正確性の原則は、関連する処理の性質及び目的を考慮して適用されなければならない。殊に司法手続において、個人データを含む供述調書は、自然人の主観的知覚に基づいており、必ずしも検証可能なものではない。結果的に、正確性の必要性は、供述調書の正確性に関連してではなく、単に特定の供述調書が作成されたという事実に関連して要求される。

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) 異なるカテゴリーのデータ主体に関する個人データが処理されることは、刑事事件における司法共助及び警察協力の分野における個人データ処理に本来的に生じるものである。それゆえ、被疑者、犯罪行為で起訴された者、犠牲者及び証人のようなその他の当事者、関連情報を持っている者、窓口となる者、容疑者の仲間及び有罪判決を受けた犯罪者のような異なるカテゴリーのデータ主体間について、当てはまる場合、可能な限りにおいて明確な区別がなされるべきである。このことは、司法裁判所及び欧州人権裁判所によるそれぞれの判例法によって形成された解釈によって憲章及び ECHR により保障されている無罪推定の権利の適用を妨げるものであってはならない。

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) 管轄を有する機関は、不正確で不完全でもはや最新ではない個人データが転送されたり利用できたりしないようにしなければならない。自然人の保護、他者に送信または利用させる個人データの正確性、完全性又はどの程度アップデートされているかを確保するため、管轄を有する機関は、可能な範囲で、送信する全ての個人データに必要な情報を加えなければならない。

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) 本指令が加盟国の法律、法的基盤又は立法措置に言及する場合、このことは、関連する加盟国の憲法上の要求に従った必要性に影響を与えることなく、必ずしも議会によって採択された立法を必要とするものではない。しかしながら、そのような加盟国の法律、法的基盤又は立法措置は、司法裁判所及び欧州人権裁判所の判例法により要求されるように、明確で、正確で、影響を受ける者にとって適用されるか否か予見可能性があるものでなければならない。本ディレクティブの射程において個人データの処理を規律する加盟国の法律は、少なくとも、目的、処理される個人データ、処理の目的、個人データの統合性及び秘密性を保持する手続、消去の手続を特定し、それゆえ、濫用及び恣意的利用のリスクに対する十分な保証を定めていなければならない。

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 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) 公共の安全に対する脅威への安全措置及び予防を含む犯罪行為の予防、捜査、検知若しくは公訴又は刑罰の執行目的で行われる、所轄官庁による個人データの処理は、自動処理であってもそうでなくても、収集、記録、組織化、構成化、保管、翻訳、修正、修復、参照、利用、整列または結合、処理の制限、確実化または破壊の目的で個人データや個人データ群に行われるいかなる作業または一連の作業を含まなければならない。特に、本指令の規定は、本指令の対象となる者から対象とならない受領者への個人データの移

転に適用されなければならない。そのような受領者は、所轄官庁により個人データが合法的に明らかにされた、自然人、法人、公的機関、省庁またはいかなる主体も含むものである。所轄官庁により、本指令にある一つの目的で最初に収集された個人データであっても、本指令の目的以外で、EU または加盟国の法により権限を与えられた目的による個人データの処理に対しては、Regulation (EU) 2016/679 が適用されなければならない。特に、Regulation (EU) 2016/679 の規定は本指令の射程外の目的での個人データの移転に適用されなければならない。所轄官庁ではなく、もしくは本指令の意味の範囲内で同様に活動していない機関が個人データの受領者として行う個人データの処理や、所轄官庁により合法的に開示された個人データに対しては、Regulation (EU) 2016/679 が適用されなければならない。本指令にしたがうだけでなく、加盟国はさらに Regulation (EU) 2016/679 の規則の条件に適合していることを具体的に述べなければならない。

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) 本指令の下での個人データの処理は、合法的であるために、犯罪の予防、捜査、取調べ検知若しくは起訴、又は刑罰の執行、さらに公共の安全に対する安全措置と脅威の防止の目的のために、EU 法または加盟国の法律に基づく所轄官庁により、公共の利益のために行われなければならない。これらの活動は、データ主体の重要な利益の保護を含まなければならない。犯罪の予防、捜査、取調べ検知若しくは起訴という法律によって所轄官庁に制度的に与えられた任務の活動は、自然人に対し、要請に応じるよう求めまたは命令することができる。このような場合、規制 (EU) 2016/679 に規定されているデータ主体の同意は、所轄官庁による個人データ処理の法的根拠とはならない。データ主体が法的義務を遵守することを求められる場合、データ主体は真の自由な選択をすることができず、データ主体の反応は、データ主体の希望がそのまま表示されたものであると扱われてはならない。これは、犯罪捜査における DNA 検査や刑罰の執行としての電子

タグによる所在の監視など、データ主体がこの指令の目的のために自分の個人データの処理に同意することを加盟国が法律によって規定することを妨げるものではない。

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) 加盟国は、送信する所轄官庁に対して EU または加盟国の法律が、処理コードを扱うなど個人データの処理に特定の状況で適用される特定の条件で適用される場合、送信する所轄官庁は、受信者に対し、それらの条件やそれらを尊重すべき要請について案内しなければならない。そのような条件は、例えば、個人データの他者へのさらなる送信、受信者へ送信された目的以外での個人データの利用、所轄官庁への事前の承認なしに送信されない権利の制限をデータ主体に伝えることの禁止などを含む。これらの義務は、送信する所轄官庁による第三国または国際機関の受信者への転送にも適用される。加盟国は、その加盟国内の所轄官庁の同様のデータ移転に適用される条件を除き、他の加盟国の受領者、または TFEU のタイトル V の第 4 章および第 5 章に従って設立された機関、事務所、および団体にそのような条件を適用しないようにする必要がある。

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) 生来、基本的人権及び自由に関して特にセンシティブな個人データは、基本的人権と自由に対する重大なリスクを生み出す処理からの特別な保護に値する。　　これらの個人データには人種や民族的出自を明らかにする個人データも含まれ、本指令における「人種的起源」という用語は、別に人種の存在を決定しようとする EU の理論の受入れを意味しない。そのような個人データは、処理が法律によって定められたデータ主体の権利および自由に対する適切な安全措置の対象となり、法律で承認された場合に許可された場合、またはそのような法律によってまだ承認されていない場合はデータ主体または他の者の重大な利益が保護される場合、またはデータ主体によって明らかに公表されているデータに関する処理の場合でなければ処理されてはならない。データ主体の権利と自由に対する適切な保護手段には、関係する自然人に関する他のデータとの関連でのみそれらのデータを収集する可能性、適切に収集されたデータを保護する可能性、所轄官庁のアクセスに関するデータに対する権限およびそれらのデータの送信の禁止についての厳格なルールを含む。そのようなデータの処理は、データ主体が特にその者にとって邪魔になる処理に明示的に同意している場合には、法律によっても許可されるべきです。しかしながら、データ主体の同意が、所轄官庁によってそのような機密の個人データを処理するための法的根拠となるべきではない。

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 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) データ主体は、自動処理のみに基づき、データ主体に有害な法的効果をもたらし、もしくは重大な影響を与える、その個人的な側面を評価する決定を条件とされない権利を有しなければならない。いかなる場合においても、そのような処理は、データ主体への特定の情報の提供、特にその者の視点を表現することを含む人間の介在を得る権利、そのような評価の後に説明を受ける権利、決定を争うための権利を含む安全措置の対象とならなければならない。基本的な権利と自由に関して特に敏感である個人データに基づいて、自然人に対する差別をもたらすプロファイリングは、憲章の 21 条および 52 条で定められた条件の下で禁止されなければならない。

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) データ主体が権利を行使するために、情報の提供は、管理者のウェブサイト上も含めて容易にアクセス可能で、明確でわかりやすい言語を用いた理解しやすいものでなければならない。そのような情報は、子どものような弱者が必要とするものでなければならない。

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) 手順は、要求の方法や、要求が認められた際には、無償で、個人データへのアクセス、訂正または消去、もしくは処理の制限含む、この指令に従って適用された規定のもとでデータ主体の権利の行使を容易にするものでなければならない。管理者は、本指令に従ってデータ主体の権利に制限を適用しない限り、過度に遅滞なくデータ主体の要求に対応する義務を負う。さらに、データ主体が不当かつ反復して情報を要求する場合、またはデータ主体が情報を受け取る権利を濫用する場合など、要求が明らかに根拠のないものまたは過度なものである場合、管理者は、合理的な料金を請求するか、または要求に応じて行動することを拒否することができる。

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) データ主体の身元を確認するために必要な追加情報の提供を管理者が要求する場合、その情報はその特定の目的のためにのみ処理されなければならず、その目的のために必要以上に長く保存されてはならない。

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) 少なくとも以下の情報がデータ主体に利用可能にされるべきである：管理者の身元、処理操作の存在、処理の目的、苦情を申し立てる権利および管理者から要求する権利の存在 個人データへのアクセスおよび訂正または消去、あるいは処理の制限。これは管轄当局のウェブサイトで行われる可能性がある。さらに、特定の場合には、またはその人の権利の行使を可能にするために、そのようなさらなる情報がある限り、データ主体は処理の法的根拠およびデータが保存される期間を知らされなければならない。データ主体に関して公正な処理を保証するために、データが処理される特定の状況を考慮する必要がある。

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) 自然人は、自分自身に関して収集されたデータにアクセスし、処理の合法性を認識し検証するために、この権利を容易かつ妥当な間隔で行使する権利を持つ。自然人は、自分自身に関して収集されたデータにアクセスし、処理の合法性を認識し検証するために、この権利を容易かつ妥当な間隔で行使する権利を持たなければならない。自然人は、自分自身に関して収集されたデータにアクセスし、処理の合法性を認識し検証するために、この権利を容易かつ妥当な間隔で行使する権利を持たなければならない。そのような通信に個人データの出自に関する情報が含まれている場合、その情報は自然人、特に機密情報の身元を明らかにしてはならない。そのような権利が守られるために、データ主体が理解可能な形式、すなわちそのデータ主体がそれらのデータを認識し、データが正確でかつ本指令にしたがって処理されていることを検証可能にする形式の、それらのデータの完全な要約を所有していることが必要であり、それにより、本指令により彼または彼女に与えられた権利を行使することが可能となる。そのような要約は、処理がなされている個人データのコピーの形で提供され得る。

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 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) 加盟国は、関係する自然人の基本的権利及び正当な利益を十分に考慮した民主主義社会において必要で均衡のとれた方法である限り、公務上又は法律上の照会、捜査又は手続の妨害を回避するため、犯罪行為の予防、捜査、探知若しくは起訴又は刑事罰の執行を害することを回避するため、公共の安全または国家の安全を守るため、又は他者の権利及び自由を保護するために、データ主体に対する情報の提供を遅らせ、制限し、除外し、もしくは全体的または部分的に個人データへのアクセスを制限する立法措置を採択することができる。管理者は、それぞれの事例において、アクセス権が部分的または完全に制限されるかについての、確実かつ個別の調査により、評価しなければならない。

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) 原則として、アクセスの拒絶又は制限は、データ主体に対し、書面により行われなければならず、判断の根拠となる事実上または法律上の理由を含んでいなければならない。

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) データ主体の権利に対する制限は、欧州司法裁判所及び欧州人権裁判所のそれぞれの判例法による解釈にしたがって欧州連合基本権憲章及び欧州人権条約を順守したものでなければならず、とりわけ、それらの権利及び自由の本質を尊重したものでなければならない。

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) 自然人は、自己に関する不正確な個人データ、特に事実に関するデータを訂正してもらう権利及び本指令に反する処理を取り消す権利を有する。しかし、例えば、訂正権は目撃証言の内容には影響しない。また、自然人は、同人が個人データの正確性に異議を唱えているものの、それが正確か不正確かを確認できない場合、または証拠として個人デ

ータを保存しておかなければならない場合には、データ処理を制限するよう求める権利も有する。特に、個別の事例において、消去がデータ主体の合理的な利益に影響を及ぼすと信じられる合理的理由がある場合には、個人データを消去する代わりに処理が制限されるべきである。そのような場合には、制限された情報は、消去を妨げることにした目的のためだけに処理される。個人データの処理を制限する方法は、とりわけ、選択された情報を、例えばアーカイブ目的の他の処理システムに移動する、または選択された情報を使用できなくすることなどである。自動ファイルシステムにおける処理の制限は、原則として、技術的手段により確保されていなければならない。個人データの処理が制限されているという事実は、システム内において、個人データの処理が制限されていることが明白にわかるよう表示されなければならない。そのような個人データの訂正、消去または処理の制限は、情報開示先の受領者と、不正確な情報をもたらした所轄官庁に伝えられなければならない。管理者は、そのような情報のさらなる流布を避けなければならない。

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) 管理者がデータ主体の情報に対する個人データへのアクセス、訂正または消去、もしくは処理の制限の権利を否定した場合、データ主体は国家の監督機関に対し、処理の適法性を検証するよう要請することができる。データ主体は、その権利について告知されなければならない。監督機関がデータ主体のために活動した場合、当該データ主体は、少なくとも、監督機関がすべての必要な検証と再検証を行ったことを監督機関から知らされる。また、監督機関は、データ主体に対し、司法的救済を受ける権利についても知らせなければならない。

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) 個人データが犯罪捜査や犯罪に関する裁判手続において処理された場合、加盟国は、個人データへのアクセス、訂正または消去、もしくは処理の制限といった情報に関する権利の行使は、司法手続に関する国家の法令に従って実行される旨定められなければならない。

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) 管理者により、または管理者のために行われた個人データの処理についての責任が、確立されなければならない。特に、管理者は適切かつ効果的な措置を実施しなければならず、処理にかかわる行動が本指令に従っていることを証明できるようにしなければならない。そのような措置は、処理の性質、範囲、状況及び目的、並びに自然人の権利及び自由に対するリスクを考慮に入れたものでなければならない。監理者がとる措置は、子どものように傷つきやすい自然人の個人データの取り扱いに配慮した特別な安全措置の策定と履行を含むものでなければならない。

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) 自然人の権利と自由に対するリスクが生じる見込みと重大性は、殊に、次に記載する物的、有形無形の損害を引き起こすデータ処理によってもたらされる：すなわち、処理が、差別、なりすまし、詐欺、財産上の損害、名誉毀損、守秘義務で保護されている個人データの秘匿性の喪失、承認のない匿名化の復元、その他重大な経済的または社会的損失をもたらす場合；データ主体が権利と自由または個人データに対するコントロールの行使を奪われる場合；人種や民族的起源、政治的意見、宗教、哲学的信念、労働組合の所属を明らかにする個人データが処理される場合；個人を特定するために遺伝情報または生物測定情報が処理される場合、健康に関する情報、性生活及び性的指向、有罪歴及び違反歴又は関連する安全措置を処理する場合；個人の容貌を評価する場合、殊に個人のプロフィールを作成または利用するために、業務成績、経済状態、健康、個人の嗜好または興味、信頼性または行動、所在又は動きを分析及び予測する場合；特に子供など、傷つきやすい自然人の個人データを処理する場合、または処理に大量の個人データが含まれ、その影響が多くのデータ主体に及ぶ場合である。

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 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) リスクが生じる見込みと重大さは、処理の性質、範囲、状況及び目的を参照して決定されなければならない。リスクは、データ処理の運用が高リスクにかかわるかどうかの客観的な評価を基礎として評価されなければならない。高リスクとは、データ主体の権利と自由に対すると特定の権利侵害のリスクである。

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) 個人データの処理に関する自然人の権利と自由の保護は、本指令の要求を遵守させるために適切な技術的、組織的な手段がとられることを必要とする。そのような手段の実施は、単に経済的な状況だけに依拠してはならない。この指令の遵守を説明できるようにするために、管理者は、殊に制度構築段階でのデータ保護及び初期設定でのデータ保護の原則に、適合した内部指針を採用し、それに従った方法を履践しなければならない。監督者が、この規則に準じるデータ保護影響評価を行う場合、その結果は個人データ処理の方法や手順の改善の際に考慮されなければならない。特に匿名化はできるだけ早く行われなければならない。本規則における匿名化の利用は、特に自由で安全で公正な領域内での個人データの流通を促進する道具として機能する。

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) データ主体の権利と自由の保護は、管理者と処理者の責任と信頼と同様に、監督機関の監視や基準とも関連して、管理者が他の管理者と共同で処理する目的と意味を決める場合または管理者のために処理する場合を含めて、この指令に示された責任の所在を明確にすることを要求する。

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) 処理者による処理は、法令により規定されなければならない。管理者に対して処理者を拘束する契約を含めて、殊に、処理者は、管理者の指示にしたがってのみ行動しなければならないよう規定していなければならない。

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) この規則の順守を証明するために、管理者又は処理者は、その責任下にあるすべての区分における処理活動に関する記録を保管しなければならない。各管理者と処理者は、監督機関に協力し、それらの記録がデータ処理作業のモニタリング機能を果たすよう、監督機関から要求があった場合にはそれらを利用できるようにする。個人データの非自動処理システムの管理者または処理者は、ログ又は他の形態の記録のように、処理の合法性、処理、自己監視ができる方法、情報の完全性及び安全性を確保できる方法を整えておかなければならない。

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) ログは、移転、結合または削除を含む、収集、選択、分析、開示、といった自動処理システムの運用について保存されなければならない。個人データを調べまたは開示した個人を特定する情報は記録されなければならず、その個人の特定情報から、処理作業の正当性を確立することができるようになっていなければならない。ログは、処理の合法性

の検証、自己モニタリング、情報の一体性、安全性刑事訴訟手続の確保のためだけに使うことができる。自己モニタリングは、所轄機関の内部的な懲戒手続を含む。

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) データ保護影響評価は、情報の性質、範囲、目的が理由で処理作業がデータ主体の権利と自由にとって高リスクがあるとの結果になりそうな場合に、管理者によって行われ、それには、特に個人データの保護を確実にし、この指令の遵守を証明するために考えられる手段、安全措置、メカニズムが含まれる。影響評価は、適切なシステムと処理作業の過程を網羅しなければならないが、個別の事例は含まない。

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.

(59) データ主体の権利及び自由の効果的な保護を確保するため、管理者又は処理者は、一定の事案では、監督機関に対し処理の前に相談しなければならない。

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) セキュリティの維持及びこの指令に反する処理を防止するため、管理者又は処理者は、当該処理に伴う危険性を評価しそれらの危険性を軽減する暗号化などの手段を取らなければならない。それらの手段は、秘匿性並びに最新技術、危険性に関連した措置の実装コスト及び保護されるべき個人データの性質の考慮を含め、適切なセキュリティのレベルが確保されなければならない。セキュリティのリスクの調査においては、データ処理により生じるリスク、例えば移転、蓄積、その他処理された個人データの偶発的若しくは違法な破壊、喪失、改変又は承認のない開示若しくはアクセス、特に有形・無形の損害を生じさせうるもの、を考慮しなければならない。管理者及び処理者は承認されない者によって個人データの処理が行われないようにしなければならない。

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) 個人データの侵害は、適切に及び適時に対処されなければ、自然人に対して、有形・無形の損害、例えば彼らの個人データへのコントロールの喪失又は権利の制限、差別、なりすまし、詐欺、財務上の損失、承認のない仮名の復元、名誉棄損、守秘義務で保護されている個人データの秘匿性の喪失又はその他当該自然人の経済的社会的損失を生じさせうる。したがって、管理者は、個人データの侵害に気が付いたらすぐに、不当に遅滞することなく、監督機関へ当該侵害を通知しなければならず、管理者が個人データの侵害が自然人の権利及び自由にリスクを生じさせるおそれがないことを説明責任の原則に従って示すことができる場合を除き、可能な限り、気づいてから 72 時間以内に監督機関へ当該侵害を通知しなければならない。72 時間以内にそのような通知ができない場合は、更なる不当な遅滞のない期間における通知及び情報に遅滞の理由を添えなければならない。

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) 自然人は、自然人の権利及び自由に対する高度の危険性を生じる可能性が高い場合、必要な対策を取ることができるよう、不当に遅滞することなく知らされなければならない。連絡は個人データの侵害の性質及び当該自然人に対して考えられる悪影響を軽減するための推奨事項を述べるものでなければならない。データ主体への連絡は、監督機関及び監督機関又は他の関係機関により提供される関連する助言の緊密な連携の下、合理的可能な限り速やかに行われなければならない。例えば、差し迫った損害の危険性を軽減する必要がある場合はデータ主体に速やかに連絡する必要があり、一方で継続中又は同種のデータ侵害に対する適切な対策については連絡までにより時間がかかることが正当化される。当該自然人へのデータ侵害の通知を遅らせ又は制限しても、公務上又は法律上の照会、捜査又は手続の妨害を回避すること、刑法犯の防止、拘禁、捜査若しくは起訴又は刑法上の罰金の執行を害することを回避すること、公共の安全を保護すること、

国家の安全を保護すること又は他者の権利及び自由を保護することが達成できない場合には、これを省略することができる。

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) 管理者は、加盟国が裁判所及び他の独立の司法機関がそれらの司法権限を行使している場合を除外することを決定したときを除いて、この指令に沿った規定の組織内部における遵守状況を監視することについて、管理者を補助する者を指定しなければならない。その者は、データ保護の法律及び実務の分野で専門的知識を得るように特別の訓練を受けた管理者の既存のスタッフをもって充てることができる。専門知識の必要なレベルは、特に、実際に処理が行われているデータ及び管理者により処理されている個人データに要求される保護によって定まる。その者の任務遂行はパートタイムでもフルタイムでもよい。一人のデータ保護担当者は、組織的構成及び規模を考慮して、例えば中央組織を設けて経営資源を共有している場合など、複数の管理者により共同して指名されることができる。その者はまた、関連する管理者の組織構成内において異なる地位に就くこともできる。その者は、個人データを取り扱う管理者や従業員に対し、関連するデータ保護義務の情報提供及び助言をすることで、彼らを助けなければならない。そのようなデータ保護担当者は、加盟国法に従って独立した方法で彼らの義務及び任務を遂行する立場でなければならない。

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) 加盟国は、第三国又は国際的組織への移転は、公共の安全に対する脅威への安全措置保護活動及び予防活動を含む、犯罪の予防、捜査、取り調べ若しくは起訴、又は刑罰の執行に必要であり、かつ当該第三国又は国際的組織の管理者がこの指令の要求を満たす機関である場合に限り行われることを保証しなければならない。移転は、処理者が明示的に管理者に代わって移転を行うことを指示されていない限り、管理者として行動している所轄官庁のみにより行われなければならない。そのような移転は、委員会が当該第三国又は当該国際的機関が十分なレベルの保護を確保していると決定した場合、適切な保護措置が提供されている場合又は特別な状況における例外が適用される場合に許される。個人データが EU から第三国又は国際的組織の管理者、処理者又は他の受領者に移転された場合、個人データが当該第三国又は国際的組織からさらに同国内若しくは同組織内又は他の第三国又は国際的組織の管理者又は処理者に移転される場合を含め、この指令により EU において自然人に提供されている保護のレベルが弱められてはならない。

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 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) 加盟国から第三国又は国際的組織に個人データが移転される場合、そのような移転は、原則として、加盟国が当該データの入手元から当該移転の承認を得た後だけに行われなければならない。効率的な法執行の協力の利益の要請から、加盟国若しくは第三国の公共の安全又は加盟国の本質的利益への脅威の性質が適時に事前の承認を得ることが不可能であるほど差し迫ったものである場合には、所轄官庁が、事前の承認を得ずに、関係する個人データを関係する第三国又は国際的組織に移転することができなければならない。加盟国は、移転に関する特定の条件が第三国又は国際的組織に伝達されなければならないことを規定しなければならない。個人データの更なる移転は元の移転を行った所轄官庁の事前の承認を受けなければならない。元の移転を行った当該所轄官庁は、更なる移転の承認の要請に関する決定を行う際には、犯罪行為の重大性、元のデータ移転の際の特別な条件及び目的、刑罰の執行の性質及び条件、並びにさらに移転される第三国又は国際的組織における個人データの保護のレベルを含む関連要素を十分考慮しなければならない。元の移転を行った所轄官庁は、転送に対して特別な条件を付するこ

とができなければならない。そのような特別な条件は、例えば、処理コードを用いて述べることができる。

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) 委員会は、EU 全体に効力を持つものとして、特定の第三国、第三国内の地域又は１つ若しくは複数の特定の部門、又は国際的組織が、十分なデータ保護のレベルを提供していることを決定でき、これによって、十分なレベルの保護を提供していると考えられる当該第三国又は当該国際的組織に関して、EU 全体にわたり法的確実性及び統一性を与える。そのような場合には、それらの国に対する個人データの移転は、当該データの入手元である他の加盟国が当該移転の承認をしなければならないときを除き、特別な承認を得ることなく行うことができる。

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) 委員会は、EU が存立する基本的価値、特に人権保護に沿って、第三国又は第三国内の地域若しくは特定の部門の調査に当たり、国際的な人権の基準並びに当該第三国の一般法及び個別法（公の秩序及び刑法と同様に、公共の安全、防衛及び国家安全保障に関する立法を含む）のみならず、当該第三国における法の支配及び司法へのアクセスの尊重の程度を考慮に入れなければならない。第三国の地域又は特定の部門に関して十分性の認定をするにあたっては、第三国における特定の取扱い及び適用されうる有効な法的基準及び立法の範囲のような明確かつ客観的な基準を考慮しなければならない。第三国は、

特にデータが１つ又は複数の特定の部門で処理される場合には、EU 内の保障と基本的に同等の十分なレベルの保護の確保を保証しなければならない。特に第三国は、効果的な独立のデータ保護の監督機関を保証し、加盟国のデータ保護当局との協力の仕組みを用意しなければならず、データ主体は効果的で執行可能な権利並びに効果的な行政的及び司法的救済を与えられなければならない。

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) 第三国又は国際的組織が参加する国際的な協定とは別に、委員会は第三国又は国際的組織の多数国間又は地域のシステムへの参加から生じる義務について、特に個人データの保護に関して、義務の実施と同様に考慮しなければならない。特に、1981 年 1 月 28 日の個人データの自動処理に関する個人の保護のための欧州評議会条約及び追加議定書への加入が考慮されなければならない。委員会は、第三国又は国際的組織における保護のレベルを調査する際には、規則（2016/679）（GDPR）により設立された欧州データ保護会議に相談しなければならない。委員会はまた、関連するすべての規則（2016/679）45 条に従って採択された委員会の十分性決定も考慮しなければならない。

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 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) 委員会は、第三国、第三国内の地域若しくは特定の部門、又は国際的組織における保護のレベルに関する認定の機能を監視しなければならない。委員会は、その十分性の認定において、機能の定期的な検査の仕組みを定めなければならない。定期検査は、当該第

三国又は国際機関と協議して実施されなければならず、当該第三国又は国際機関におけるすべての関連状況を考慮しなければならない。
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) 委員会は、第三国、第三国内の地域若しくは特定の部門又は国際組織が、データ保護について十分なレベルを維持していないことにつき判断できなければならない。この結果、個人データの当該第三国又は国際組織への移転は、移転に関する本指令の要件（適切な安全措置と特定の状況における例外的な条件に従う）を満たさない限り、禁止されなければならない。委員会と当該第三国又は国際組織の間で行われる協議に関する手続規定が定められなければならない。委員会は、遅滞なく、当該第三国又は国際組織に対し理由を告げたうえで、状況改善のために協議に入らなければならない。

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) 十分性の認定に依拠しない移転は、適切な安全措置が、個人データの保護を確実にする法的拘束力のある法律文書に基づき設けられている場合、又は管理者が、当該データ移転に関するあらゆる状況を査定し、かつ当該査定に基づき個人データの保護に関する適切な安全措置が存在すると判断した場合に限り、許容される。当該法的拘束力のある法律文書は、例えば、データ保護と、効果的な行政・司法的救済を含むデータ主体の権利保護を確実に満たし、データ主体の加盟国により締結され、かつ加盟国の法的な命令によって実行されたもの、もしくはデータ主体によって援用されうる、法的拘束力のある二国間合意である。管理者は、データ移転に関するあらゆる状況の査定が実施される際に、個人データの移転を許諾した第三国と、欧州警察または欧州司法機構との間で締結された協力合意を考慮し得なければならない。管理者は、個人データの移転が守秘義務及び特異性の原則、すなわち当該データ移転の目的以外の目的には個人データが使用されることはないという原則に基づき実施されるという事実もまた考慮しなければならない。加えて、管理者は、個人データが死刑又はその他の残虐で非人道的な取り扱いの求刑、判決言い渡し又は執行に利用されてはならないことも考慮しなければならない。これらの条件は個人データの移転を許容する適切な安全措置として考慮されうる一方、管理者は、さらなる安全措置を求めることができなければならない。

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) 十分性判断又は適切な安全措置の存在が認められない場合には、データ移転又はカテゴリー移転は特別な状況下においてのみ許容される。すなわち、データ主体または他者の非常に重要な利益を守るため、又は移転元の加盟国の法律が求めるデータ主体の正統な利益を保護するために必要な場合；加盟国または第三国の即時かつ重大な治安上の脅威を防ぐため；個別の事例において、公共の治安に対する脅威の予防を含む、刑事犯罪の予防、調査、捜査もしくは起訴又は刑罰の執行のため；個別の事例において法的要求を確立、執行又は防御するため。これらの例外は、厳格に解されなければならない。度重なる、大量の、かつ構造的なデータ移転、又は大規模なデータ移転に認められてはならず、厳格に必要なデータのみに限定されなければならない。当該移転は、文書によってなされなければならず、移転の適法性を検証するため必要に応じて監督機関の審査に服さなければならない。

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) 加盟国の所管官庁は、法的に与えられた職務を遂行するための関連情報を交換するため、刑事事件における司法共助および警察協力において第三国と締結された二国間また

は多国間の強制力ある国際協定を適用できる。原則として、当該適用は、ときには当該二国間または多国間国際協定が存在しない場合において、少なくとも、当該第三国の本指令の目的に関連する管轄機関の協力を通じて実施される。しかしながら、特別な事例においては、特に当該移転が時機に即して実施され得ない場合や、当該第三国の監督機関が法の支配、または国際人権に関する規範もしくは水準を尊重していない場合など、当該第三国の管轄機関と接触する正規の手続きが効果的でなく、また不相当な場合がある。このような場合、加盟国の所管官庁は、個人データを直接、当該第三国に設置された受取人に送付することを決定することができる。刑事事件の被害者に今まさになろうとしている個人の生命を防ぐため、またはテロを含む切迫した犯罪実行を予防する利益のために個人データを移転する緊急の必要がある場合などに認められうる。たとえ特別な個別事例においてのみ所管官庁と第三国に設置された受取人の間の移転が行われるとしても、本指令は当該事例を規律する条件を提示しなければならない。当該条項は、刑事事件における司法共助および警察協力において現存する二国間または多国間の国際協定の逸脱と考えられるべきではない。当該条項は、とりわけ処理の適法性および第５章などの、本指令の他の条項に付加されるものとして適用するべきである。

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 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) 個人データが国境を越えると、当該データの違法な利用または漏洩から自身を保護するためにデータ保護の権利を行使する自然人の能力に対するリスクを増加することになりうる。同時に、監督機関は、国境外の出来事に関して苦情を申し立てたり、調査を遂行することが不可能であることを理解するかもしれない。国境を超えた文脈における共同作業の努力は、予防的または救済的権限の不十分さや一貫性のない法体制によって阻まれるかもしれない。それゆえ、関係国の監督機関と情報交換する手助けをするために、データ保護の監督機関相互により密接な協力を推進する必要がある。

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) 加盟国において完全に独立してその機能を果たすことができる監督機関を設立することは、個人データを処理される自然人の保護において本質的な構成要素である。監督機関は、本指令に基づき採択される条項の適用を監督するべきであり、また個人データを処理される自然人を保護するために EU 全域で本指令が整合的に適用されるよう貢献するべきである。当該目的のために、監督機関は相互にまた委員会と、協力するべきである。

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) 加盟国は、EU 規則 2106/679 に基づきすでに設立された監督機関に、本指令に基づき設立される国内の監督機関が遂行すべき職務を委嘱することができる。

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) 加盟国は、自国の憲法的、組織的、そして行政的な構造に即して、1 つ以上の監督機関を設立することができる。各監督機関は、EU 域内における他の監督機関との相互扶助や相互協力を含む、その職務を効果的に遂行するために必要な、財政的および人的資源、施設並びに基盤が与えられなければならない。各監督機関は、全州または国家予算の一部を構成する、独立かつ公的な年間予算が与えられなければならない。

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) 監督機関は、財政的な支出に関し、独立の統制または監視の仕組みに服さなければならない。ただし、当該財政的な統制は、監督機関の独立性に影響を及ぼすものであってはならない。

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) 加盟国または監督機関の一員たる一般的な条件は、加盟国の法律によって制定されなければならず、特にその構成員は、政府もしくは政府のメンバー、国会または立法機関の一部、加盟国の国会または政府または元首、加盟国の法律に基づき透明性のある手続による任命を委託された独立機関によって任命されるべきである。
監督機関の独立性を確保するため、構成員は、尊厳を持って行動しなければならず、職務に反するいかなる言動も慎み、任期中、有償であれ無償であれ、職務に反する職業についてはならない。監督機関の独立性を確保するため、職員は、加盟国の法律によって委託された独立機関による認証は含めてもよいが、監督機関によって選任されなければならない。

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) 本指令は、国内裁判所その他の司法機関の活動にも適用される一方、司法権の行使における裁判官の独立性を保護するため、監督機関の管轄は、裁判所が司法権の範囲内で行った個人データの処理に及ぶものではない。当該例外は、法廷内における司法権の行使に限られ、裁判官が加盟国の法律に基づき関与する可能性のある他の活動には適用されない。加盟国は、例えば公的な検察官の事務所など司法領域における活動に関して、監督機関の管轄を、他の独立した司法機関の個人データの処理に及ばせないことができる。いかなる場合においても、裁判所及び他の独立した司法機関による本指令の規則の遵守は、常に、本章 8 条(3)に基づく独立した監督にさらされる。

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.

(81) 各監督機関はデータ主体が申し立てた苦情に対処し、当該事案を調査するか、または所轄の監督機関に送らなければならない。苦情に関する調査は、当該事案に適切な範囲で司法審査に服するべきである。監督機関は、データ主体に対し、合理的な期間内に、苦情についての進捗及び結果を知らせなければならない。当該事案についてさらなる調査又は他の監督機関との調整を必要とする場合は、データ主体に対して中間的な報告をしなければならない。

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) 欧州司法裁判所の解釈による EU 機能条約に従い、EU 全体における本指令の遵守及び実施を効果的確実かつ整合的にモニタリングすることを確保するため、監督機関は、各加盟国において同様の任務を遂行し、これらの任務を遂行するために必要な手段である調査、是正及び監督の権限を含む有効な権限を有しなければならない。しかしながら、これらの権限は、刑事犯罪の捜査及び起訴を含む刑事手続固有のルールや司法の独立を妨げてはならない。各加盟国の法に基づく検察当局の権限を侵害することなく、監督機関も、本指令の違反を司法当局に提起したり、法的手続に関与したりする権限を有するべきである。監督機関の権限は、EU 及び各加盟国の法が定める適切な手続上の保護措置に従い、公平・公正に、かつ合理的な期間内に行使されるべきである。特に、それぞれの手段は、本指令の遵守を確保するために適切、必要かつ比例的なものでなければならず、各事案の状況を考慮し、関係者に不利益を与える手段が採られる前にその者の意見聴取を受ける権利を尊重し、関係者に過度に不便を強いることや余分なコストを避けなければならない。施設に対するアクセスに関する調査権は、司法当局より事前に許可を得ることなど、加盟国の法の定める具体的な要件に従って行使されるべきである。法的拘束力のある決定は、当該決定を行った監督機関の加盟国における司法審査に服さなければならない。

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) 監督機関は、任務を遂行する上で、本指令に基づき採択された規定の整合的な適用及び実施を確保するために、互いに協力し、支援し合う。

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) 欧州データ保護会議は、委員会への助言や、EU 全体における監督機関の協力を促すことを含め、EU 全体への本指令の整合的な適用に貢献しなければならない。

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) 各データ主体は、本指令に基づき採択された規定に基づく彼らの権利が侵害されたと考える場合、又は監督機関が苦情に対応せず、苦情の全部若しくは一部を拒否若しくは却下し、若しくはデータ主体の権利を保護するために必要な行動を取らない場合は、単一の監督機関に苦情を申し立てる権利、及び欧州連合基本権憲章 47 条に従い効果的な司法救済を得る権利を有するべきである。苦情に関する調査は、当該事案に適切な限度で司法審査に服するべきである。所轄の監督機関は、データ主体に対し、合理的な期間内に、苦情についての進捗及び結果を知らせなければならない。当該事案についてさらなる調査又は他の監督機関との調整を必要とする場合は、データ主体に対して中間的な報告をしなければならない。苦情の申出を促進するために、各監督機関は、他の通報手段を排除することなく、電子的に入力可能な苦情申出の書式を用意するなどの措置を講じなければならない。

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) 各自然人及び法人は、自身について法的効果を生じる監督機関の決定に対して、所管する国の裁判所に、効果的な司法救済を求める権利を有するべきである。こうした決定は、特に監督機関による調査、是正及び認可の権限の行使又は苦情の却下・拒絶に関わるものである。しかしながら、かかる権利は、監督機関の表明した意見や助言のような、法的拘束力のない監督機関の措置には及ばない。監督機関に対する法的手続は、監督機関が設けられた加盟国の裁判所に提起されるべきであり、加盟国の法に基づいて処理されるべきである。当該裁判所には、提起された争訟に関連するあらゆる事実及び法的論点を審理する権限を含む完全な権限が認められなければならない。

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) データ主体が、本指令に基づく自分の権利が侵害されていると考えた場合、個人データの保護に関してデータ主体の権利利益の保護を目的とする、加盟国の法に基づき設立された機関に対して、自身を代理して監督機関に苦情を申し立て、司法的救済を受ける権利を行使することを求める権限を有するべきである。代理人に委任するデータ主体の権利は、加盟国の手続法により、理事会指令 77/249/EEC が定義するように、各国の法廷においてデータ主体の弁護士による代理が義務づけられている場合も、これに影響を及ぼすものであってはならない。

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 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[10], before national courts.

(88) 本指令に従って採択された規定に違反する処理によって損害を被った者の損害は、管理者又は加盟国の法に基づき管轄を有する機関によって補償されるべきである。損害の概念は、本指令の趣旨を十分に反映し、欧州連合司法裁判所の判例法に照らして広く解釈されなければならない。このことは、EU における他の規則又は加盟国の法違反によるいかなる損害の請求にも影響を及ぼさない。違法な処理又は本指令に従って採択された規定に違反する処理とは、本指令に基づいて採択された実施行為に違反する処理を含む。データ主体は、その被った損害について完全かつ効果的な補償を受け取ることができなければならない。

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) 罰則は、本指令に違反したあらゆる自然人及び法人（私法に基づく法人であると公法に基づく法人であるとを問わない）に適用されるものとする。加盟国は、罰則が実効的かつ比例的であり、抑止力のあるものであることを確保すべきであり、罰則を実施するためのあらゆる措置を講じるべきである。

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) 本指令施行のための統一的な条件を確保するために、第三国、第三国内の領土若しくは特定の区域、又は国際機関による保護の十分性について、並びに、監督機関同士及び監督機関と欧州データ保護会議との間の相互支援の形態と手続及び電子的手段による情報交換のための手配について、委員会に実施権限が与えられなければならない。これらの権限は、EU 議会及び EU 理事会の EU182/2011 規則に従って行使される。

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

[10] 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).

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[11].

(91) 第三国、第三国内の領土若しくは特定の区域、又は国際機関による保護の十分性に関する実施行為、並びに監督機関同士及び監督機関と欧州データ保護会議との間の相互支援の形態と手続及び電子的手段による情報交換のための手配に関する実施行為を採択するにあたっては、当該実施行為が一般的な範囲のものであることから、調査手続を経るべきである。

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) 委員会は、第三国、第三国内の領土若しくは特定の区域、又は国際機関において十分な保護が確保されないという正当な理由があり、緊急の必要不可欠な理由がある場合は、即時に適用される実施行為を採択すべきである。

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) 本指令の目的、すなわち、自然人の基本権及び自由、とりわけ個人データの保護を受ける権利を守り、EU 内の所管官庁間で行われる個人データの自由な流通を確保することは、加盟国によっては十分達成することができず、当該措置の規模又は効果ゆえに、EU レベルにおいてよりよく達成できるものであることから、EU は、EU 条約第 5 条に定める補完性の原則に従い、措置を講じることができる。同条に定める補完性の原則に従い、本指令は、これらの目的を達成するために必要な範囲を超えるものではない。

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) 本指令の採択に先立って採択された、刑事事件における司法共助及び警察協力の分野

[11] 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).

における EU の法的行為の特定の規定であって、加盟国間での個人データの処理又は諸条約に基づいて設けられた情報システムへの加盟国の指定機関によるアクセスを規制するもの、例えば、EU 理事会決定 2008/615/JHA（特にテロリズム及び国境を越える犯罪との闘いにおける国境を越える協力の拡大に関する決定）又は EU 加盟国間の刑事相互協力に関する条約 23 条に基づいて適用される個人データの保護に関する規定は、影響を受けないこととしなければならない。憲章 8 条及び EU 機能条約 16 条が、個人データの保護を受ける基本権が EU において一貫して保障されることを要求していることから、EU 委員会は、本指令の採択に先立って採択された、加盟国間での個人データの処理又は諸条約に基づいて設けられた情報システムへの加盟国の指定機関によるアクセスを規制する法的行為の特定の規定を本指令に合致させる必要性を精査するために、本指令とこれらの法的行為との関係に関する状況を検討すべきである。必要に応じて、EU 委員会は、個人データの処理に関する整合的な法規制を確保するために提言をすべきである。

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 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[12], or Article 23 of the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union[13]. 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) EU 連合における個人データの包括的かつ一貫した保護を確実にするために、本指令の発効日以前に加盟国によって締結された国際協定及び同発行日以前に適用された関連する EU 法は、改正、差替え又は無効とされるまでは、有効である。

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) 加盟国は、本指令の発効日から 2 年以内の期間は、本指令への置換えを猶予される。発効日にすでに処理中のものは、本指令が発効してから、2 年以内に本指令に適合する

[12] 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).
[13] 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).

ようにしなければならない。本指令が効力を生じた日よりも前に導入された自動化された処理システムへのログ保存義務への適合について、加盟国が発行日から７年後を期限とする実施期間よりも長期の期間を要する場合は、管理者又は処理者は、データ処理の適法性を示すため、自己監視を可能にし、データの完全性及びデータの安全性を確保する、ログやその他の形式の記録のような有効な手段を採用しなければならない。

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)　本指令は、欧州議会及び理事会の Directive 2011/93/EU によって定められた、子どもの性的虐待、性的搾取及び児童ポルノと戦うための規則を害するものではない。

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[14].

(98)　枠組み決定 2008/977/JHA は廃止すべきである。

Framework Decision 2008/977/JHA should therefore be repealed.

(99)　EU 基本条約及び EU 機能条約に付加された議定書（第 21 号）（自由、安全と司法の領域に関する英国とアイルランドの地位について）第 6 a 条に従って、英国とアイルランドは、EU 機能条約 16 条に基づき定められた規定の遵守を求める犯罪の司法協力又は警察協力の形態を定める規則に英国とアイルランドが拘束されないことを定める EU 機能条約第 3 部第 5 編第 4 章又は第 5 章に規定する範囲の活動を行うときは、加盟国による個人データの処理に関する本指令に基づくルールに拘束されない。

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

[14] 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).

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) EU 基本条約及び EU 機能条約に付加された議定書（第 22 号）（デンマークの地位について）第 2 条及び第 2 a 条に従って、デンマークは、本指令の規定に拘束されず、また、EU 機能条約第 3 部第 5 編第 4 章又は第 5 章に規定する範囲の活動を行う場合において加盟国による個人データの処理に関して本指令の規定の適用を受けない。本指令は、EU 機能条約の第 3 部第 5 編の下にあるシェンゲン・アキ（シェンゲン協定に関する法的枠組み）に基づいて成立したものであるから、上記議定書第 4 条の定めに従い、デンマークは 6 か月以内に本指令を国内法として実施するかどうかについて決定することとなる。

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) アイルランド及びノルウェーについては、シェンゲン・アキの両国における実施、適用及び発展に関する両国及び EU 理事会との間の合意により規定されたように、本指令は、シェンゲン・アキの規定の発展した一部を構成する。

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*[15].

(102) スイスについては、シェンゲン・アキのスイスにおける実施、適用及び発展に関する EU、EC 及びスイスとの間の合意により規定されたように、本指令は、シェンゲン・アキの規定の発展した一部を構成することとなる。

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* [16].

[15] OJ L 176, 10.7.1999, p. 36.
[16] OJ L 53, 27.2.2008, p. 52.

(103) リヒテンシュタインについては、シェンゲン・アキのスイスにおける実施、適用及び発展に関するEU、EC、スイスとの間の合意への加入に関する、EU、EC、スイス、リヒテンシュタインとの間の議定書に定められたとおり、本指令は、シェンゲン・アキの規定の発展した一部を構成することとなる。

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*[17].

(104) 本指令は基本的権利を尊重するとともに、EU機能条約で義務付けられている憲章の原則、特に、私的・家庭生活を尊重される権利、個人データの保護の権利、効果的な救済及び公正な裁判の権利を監視する。これらの権利に関する制限は、EU が一般的利益と認める目的を達成するために必要であるか、又は他人の権利及び自由を擁護するために必要である場合に限られるとする憲章第52条1項に従う。

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) 2011年9月28日の加盟国及びEU委員会との間の共同政治宣言に基づき、加盟国は、正当な理由により、指令の構成要素と各国の移行措置の対応する部分との関係を説明する1つ以上の文書を用いて、移行措置の通知を付託することを試みた。本指令についていえば、立法者は、そのような文書による伝達が正当と考える。

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) EUデータ保護監督者は、EC規則No 45/2001第28条2項に基づいて、事前協議を受け、2012年3月7日に意見を出した。

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[18].

---

[17] OJ L 160, 18.6.2011, p. 21.

[18] OJ C 192, 30.6.2012, p. 7.

(107)　本指令は、加盟国によるデータ主体の情報に関する権利の行使、すなわち個人データへのアクセス、訂正、削除の実施や、各国の刑事手続法に定められた刑事手続に関する処理の制限ないしその制限可能性を妨げるものではない。

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,

以上の次第で、本指令を採択した。
HAVE ADOPTED THIS DIRECTIVE: