仮日本語訳

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)

個人データの取扱いと関連する自然人の保護に関する、及び、そのデータの自由な移転に関する、並びに、指令 95/46/EC を廃止する欧州議会及び理事会の 2016 年 4 月 27 日の規則(EU) 2016/679（一般データ保護規則）

【前文】

本書面は、“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)”の英語版の前文を個人情報保護委員会が翻訳したものである。本書面は参考のための仮日本語訳であって、その利用について当委員会は責任を負わないものとし、正確な内容については原文を参照されたい。また、翻訳の内容について、必要な場合には随時修正することがある点についてもご留意いただきたい。

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,
欧州議会及び欧州連合の理事会は、
Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,
欧州連合の機能に関する条約、及び、特に、同条約の第 16 条に鑑み、
Having regard to the proposal from the European Commission,
欧州委員会からの提案に鑑み、
After transmission of the draft legislative act to the national parliaments,
立法案を加盟国の議会に送付した後、
Having regard to the opinion of the European Economic and Social Committee [1],
欧州経済社会委員会の意見に鑑み[1]、
Having regard to the opinion of the Committee of the Regions [2],
地域委員会の意見に鑑み[2]、
Acting in accordance with the ordinary legislative procedure [3],
通常の立法手続に従って審議し[3]、
Whereas:
以下のとおりであるので、本規則を採択する。

(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.
(1) 個人データの取扱いと関連する自然人の保護は、基本的な権利の一つである。欧州連合基本権憲章（以下「憲章」という。）の第 8 条第 1 項及び欧州連合の機能に関する条約（以下「TFEU」という。）の第 16 条第 1 項は、全ての者が自己に関する個人データの保護の権利を有すると定めている。

(2) The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.
(2) 自然人の個人データの取扱いと関連する自然人の保護の基本原則及びそれと関連する法令は、その国籍及び居住地がいかなるものであれ、自然人の基本的な権利及び自由を尊重し、特に、その個人データ保護の権利を尊重する。本規則は、自由、安全及び正義の領域の達成及び経済共同体の達成、経済的及び社会的な成長、域内市場における経済の強化及び収斂、並びに、自然人の福利に貢献しようとするものである。

(3) Directive 95/46/EC of the European Parliament and of the Council [4] seeks to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to ensure the free flow of personal data between Member States.
(3) 欧州議会及び理事会の指令 95/46/EC[4]は、取扱活動と関連する自然人の基本的な権利及び自由の保護を整合

[1] OJ C 229, 31.7.2012, p. 90.
OJ C 229, 31.7.2012, p. 90.
[2] OJ C 391, 18.12.2012, p. 127.
OJ C 391, 18.12.2012, p. 127.
[3] Position of the European Parliament of 12 March 2014 (not yet published in the Official Journal) and position of the Council at first reading of 8 April 2016 (not yet published in the Official Journal). Position of the European Parliament of 14 April 2016.
欧州議会の 2014 年 3 月 12 日付け意見書（官報未登載）及び第 1 読会における欧州連合理事会の 2016 年 4 月 8 日付け意見書（官報未登載）及び欧州議会の 2016 年 4 月 14 日付け意見書
[4] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

性のとれたものとすること、そして、加盟国間における個人データの自由な移転を確保することを求める。

(4) The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.
(4) 個人データの取扱いは、人間に奉仕するために設計されるべきである。個人データ保護の権利は、絶対的な権利ではない；すなわち、それは、比例性原則に従い、社会におけるその機能との関係において判断されなければならず、かつ、他の基本的な権利とバランスのとれたものでなければならない。本規則は、全ての基本的な権利を尊重し、そして、憲章によって認められ、諸条約に掲げられている自由及び基本原則、特に、私的な家庭生活、住居及び通信の尊重、個人データの保護、思想、信条及び信教の自由、表現及び情報伝達の自由、事業活動を営む自由、実効的な救済及び公正な裁判を受ける権利、並びに、文化上、宗教上及び言語上の多様性を尊重する。

(5) The economic and social integration resulting from the functioning of the internal market has led to a substantial increase in cross-border flows of personal data. The exchange of personal data between public and private actors, including natural persons, associations and undertakings across the Union has increased. National authorities in the Member States are being called upon by Union law to cooperate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State.
(5) 域内市場の機能からもたらされる経済及び社会の統合は、個人データの国境を越える移転の大規模な増加を導いた。EU 全域において、自然人、団体及び事業者を含め、公的な行為主体及び民間の行為主体の間における個人データの交換が増加した。加盟国の国家機関は、EU 法によって、加盟国自身の職務を遂行できるようにするため、又は、他の加盟国の機関の代わりにその職務を行うことができるようにするため、協力すること、及び、個人データを交換することが求められている。

(6) Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data.
(6) 急速な技術発展とグローバル化は、個人データ保護に対して新たな課題をもたらした。個人データの収集及び共有の規模は、大きく増加した。技術は、私企業と公的機関のいずれに対しても、その活動の遂行のために、かつてない規模で個人データを利用できるようにしている。自然人は、個人情報を公開で、グローバルに利用できる機会を増加させている。技術は、経済と社会生活の両方を変容させ、また、高いレベルの個人データ保護を確保しつつ、EU 域内における個人データの自由な移転と第三国及び国際機関に対する移転をさらに促進しなければならない。

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

---

個人データの取扱いと関連する個人の保護に関する、及び、そのデータの自由な移動に関する欧州議会及び理事会の 1995 年 10 月 24 日の指令 95/46/EC（OJ L 281, 23.11.1995, p.31）

economic operators and public authorities should be enhanced.
(7) 域内市場全域にわたりデジタル経済を発展させることができるようにする信頼を形成することの重要性に鑑み、それらの発展は、強力な執行によって支えられた EU 域内における強力かつより一貫性のある個人データ保護の枠組みを必要とする。自然人は、自身の個人データの支配権限をもつべきである。自然人、事業者及び公的機関のための法的安定性及び実務上の確実性は、高められなければならない。

(8) Where this Regulation provides for specifications or restrictions of its rules by Member State law, Member States may, as far as necessary for coherence and for making the national provisions comprehensible to the persons to whom they apply, incorporate elements of this Regulation into their national law.
(8) 加盟国の国内法によるその法令の仕様又は制限を本規則が定める場合、加盟国は、その一貫性を保つため、及び、その法令の適用を受ける者にとって国内条項を理解しやすくするために必要がある範囲内で、本規則の諸要素を国内法の中に組み込むことができる。

(9) The objectives and principles of Directive 95/46/EC remain sound, but it has not prevented fragmentation in the implementation of data protection across the Union, legal uncertainty or a widespread public perception that there are significant risks to the protection of natural persons, in particular with regard to online activity. Differences in the level of protection of the rights and freedoms of natural persons, in particular the right to the protection of personal data, with regard to the processing of personal data in the Member States may prevent the free flow of personal data throughout the Union. Those differences may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law. Such a difference in levels of protection is due to the existence of differences in the implementation and application of Directive 95/46/EC.
(9) 指令 95/46/EC の目的及び基本原則は、今なお正しいものであるが、EU 全域における個人データ保護の実装の断片化、法的な不安定性、又は、特に、オンライン上の行為に関して、自然人の保護に対する重大なリスクがあるという一般的な認識が広がることを防止できなかった。加盟国内における個人データの取扱いに関し、自然人の権利及び自由、特に個人データ保護の権利のレベルに相違があることは、EU 全域にわたる個人データの自由な移転を妨げうる。それゆえ、それらの相違は、EU のレベルでの経済活動の遂行の障碍を構成しうるものであり、競争を歪め、そして、EU 法に基づく当局の職責遂行を害するものとなりうる。そのような保護のレベルの相違は、指令 95/46/EC の実装及び適用における相違が存在することによるものである。

(10) In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union. Regarding the processing of personal data for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Member States should be allowed to maintain or introduce national provisions to further specify the application of the rules of this Regulation. In conjunction with the general and horizontal law on data protection implementing Directive 95/46/EC, Member States have several sector-specific laws in areas that need more specific provisions. This Regulation also provides a margin of manoeuvre for Member States to specify its rules, including for the processing of special categories of personal data ('sensitive data'). To that extent, this Regulation does not exclude Member State law that sets out the circumstances for specific processing situations, including determining more precisely the conditions under which the processing of personal data is lawful.
(10) 一貫性があり高いレベルの自然人の保護を確保するため、そして、EU 域内における個人データの流通の障碍を除去するために、そのデータの取扱いと関連する自然人の権利及び自由の保護のレベルは、全ての加盟国において均等でなければならない。EU 全域において、個人データの取扱いと関連する自然人の基本的な権利及び自由の保護について法令の一貫性のある均質な適用が確保されなければならない。法律上の義務の遵守のための個人データの取扱い、公共の利益において行われる職務、又は、管理者に与えられた公的な権限の行使において行われる職務の遂行のための個人データの取扱いに関し、加盟国は、本規則の規定の適用の細則を

定める国内法上の条項を維持又は導入することが認められなければならない。指令 95/46/EC を実装する一般的で水平的なデータ保護法と併せ、加盟国は、より細かな条項を必要とする分野におけるいくつかの部門別の法律をもっている。本規則は、特別な種類の個人データ（以下「センシティブデータ」という。）の取扱いに関するものを含め、加盟国がその法令を定める余地も与えている。その範囲内で、本規則は、個人データの取扱いが適法であることの条件をより詳細に定めることを含め、特別な取扱いをする状況のための前提となる事情を定める加盟国の国内法を排除しない。

(11) Effective protection of personal data throughout the Union requires the strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States.
(11) EU 全域における個人データの実効的な保護は、データ主体の権利及び個人データを取扱う者とその取扱いを決定する者の義務を強化し、かつ、その詳細を定めること、並びに、加盟国内において個人データ保護法令の遵守を監視し、確保するための均等な権限及び違反行為に対する均等な制裁を必要とする。

(12) Article 16(2) TFEU mandates the European Parliament and the Council to lay down the rules relating to the protection of natural persons with regard to the processing of personal data and the rules relating to the free movement of personal data.
(12) TFEU の第 16 条第 2 項は、欧州議会及び欧州理事会に対し、個人データの取扱いと関連する自然人の保護に関する法令及び個人データの自由な移動に関する法令を制定することを命じている。

(13) In order to ensure a consistent level of protection for natural persons throughout the Union and to prevent divergences hampering the free movement of personal data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide natural persons in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors, to ensure consistent monitoring of the processing of personal data, and equivalent sanctions in all Member States as well as effective cooperation between the supervisory authorities of different Member States. The proper functioning of the internal market requires that the free movement of personal data within the Union is not restricted or prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data. To take account of the specific situation of micro, small and medium-sized enterprises, this Regulation includes a derogation for organisations with fewer than 250 employees with regard to record-keeping. In addition, the Union institutions and bodies, and Member States and their supervisory authorities, are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation. The notion of micro, small and medium-sized enterprises should draw from Article 2 of the Annex to Commission Recommendation 2003/361/EC [5].
(13) EU 全域において自然人のための一貫性のあるレベルの保護を確保し、かつ、域内市場内における個人データの自由な移動を妨げる格差を防止するため、中小零細企業を含む事業者に対して法的安定性と透明性を定め、全ての加盟国内の自然人に対して同じレベルの法的に執行可能な権利、そして、管理者及び処理者の義務と責任を定め、個人データの取扱いの一貫性のある監視、及び、全ての加盟国において均等な制裁、並びに、異なる加盟国の監督機関の間における効果的な協力を確保するための規則が必要である。域内市場が適正に機能するためには、個人データの取扱いと関連する自然人の保護と関係する理由によって、EU 域内における個人データの自由な移動が制限又は禁止されないことが求められる。中小零細企業の特殊事情を考慮に入れるため、本規則は、記録の保管に関し、従業員数 250 名未満の組織のための例外を含める。加えて、EU の機関及び組織並びに加盟国及びその監督機関は、本規則の適用に際し、中小零細企業の特別の必要性を考慮に入れることが推奨される。中小零細企業の概念については、委員会勧告 2003/361/EC[5]の別紙の第 2 条に規定するとお

[5] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (C(2003) 1422) (OJ L 124, 20.5.2003, p. 36).
マイクロ企業、小企業及び中規模企業の定義に関する 2003 年 5 月 6 日の委員会勧告（C(2003) 1422）（OJ L 124, 20.5.2003, p.36）

りである。

(14) The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data. This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person.
(14) 本規則によって与えられる保護は、その国籍及び居住地がいかなるものであれ、自然人の個人データの取扱いとの関係において、自然人に対して適用される。本規則は、法人の名称及び形式並びに法人の連絡先を含め、法人と関係する個人データの取扱い及び特に法人として設立された事業者と関係する個人データの取扱いをその適用対象としない。

(15) In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used. The protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system. Files or sets of files, as well as their cover pages, which are not structured according to specific criteria should not fall within the scope of this Regulation.
(15) 適用を免れる重大なリスクがつくり出されることを防止するため、自然人の保護は、技術的に中立でなければならず、かつ、用いられる技術に依存するものであってはならない。自然人の保護は、自動的な手段による個人データの取扱い、及び、その個人データがファイリングシステムに含められている場合又は含められる予定である場合には、手作業の取扱いによる個人データの取扱いに適用される。特定の基準に従って構成されていないファイル若しくは一群のファイル及びその表紙は、本規則の適用範囲内にない。

(16) This Regulation does not apply to issues of protection of fundamental rights and freedoms or the free flow of personal data related to activities which fall outside the scope of Union law, such as activities concerning national security. This Regulation does not apply to the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union.
(16) 本規則は、国家安全保障と関係する活動のような EU 法の適用範囲外にある活動と関連する基本的な権利及び自由の保護の問題並びに個人データの自由な流通の問題には適用されない。EU の共通の外交政策及び安全保障政策との関連においてその活動が行われる場合、本規則は、加盟国による個人データの取扱いに対して適用されない。

(17) 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 this Regulation and applied in the light of this Regulation. In order to provide a strong and coherent data protection framework in the Union, the necessary adaptations of Regulation (EC) No 45/2001 should follow after the adoption of this Regulation, in order to allow application at the same time as this Regulation.
(17) 欧州議会及び理事会の規則(EC) No 45/2001[6]は、EU の機関、組織、事務局及び部局による個人データの取扱いに適用される。規則(EC) No 45/2001 及びそのような個人データの取扱いに適用可能な EU の法律行為は、本規則に定める基本原則及び規定に合わせて調整されなければならず、また、本規則に照らして適用されなければならない。EU における強固かつ一貫性のあるデータ保護の枠組みを定めるため、本規則の採択の後、本規則と同時に適用できるようにするため、規則(EC) No 45/2001 の必要な調整が行われなければならない。

---

[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).
欧州共同体の機関及び組織による個人データの取扱いと関連する個人の保護に関する、及び、そのデータの自由な移動に関する欧州議会及び理事会の 2000 年 11 月 18 日の規則(EC) No 45/2001（OJ L 8, 12.1.2001, p.1）

(18) This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. Personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities.
(18) 本規則は、純粋に私的な行為又は家庭内の行為の過程における自然人による個人データの取扱いであって、職業活動又は商業活動とは何らの関係もないものには適用されない。私的な行為又は家庭内の行為は、手紙のやりとり及びアドレスの保管、又は、そのような行為の過程で行われるソーシャルネットワーキング及びオンラインの行為を含みうる。ただし、そのような私的な行為又は家庭内の行為のために個人データの取扱いの手段を提供する管理者又は処理者に対しては、本規則が適用される。

(19) The protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and the free movement of such data, is the subject of a specific Union legal act. This Regulation should not, therefore, apply to processing activities for those purposes. However, personal data processed by public authorities under this Regulation should, when used for those purposes, be governed by a more specific Union legal act, namely Directive (EU) 2016/680 of the European Parliament and of the Council[7]. Member States may entrust competent authorities within the meaning of Directive (EU) 2016/680 with tasks which are not necessarily carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and prevention of threats to public security, so that the processing of personal data for those other purposes, in so far as it is within the scope of Union law, falls within the scope of this Regulation. With regard to the processing of personal data by those competent authorities for purposes falling within scope of this Regulation, Member States should be able to maintain or introduce more specific provisions to adapt the application of the rules of this Regulation. Such provisions may determine more precisely specific requirements for the processing of personal data by those competent authorities for those other purposes, taking into account the constitutional, organisational and administrative structure of the respective Member State. When the processing of personal data by private bodies falls within the scope of this Regulation, this Regulation should provide for the possibility for Member States under specific conditions to restrict by law certain obligations and rights when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific important interests including public security and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. This is relevant for instance in the framework of anti-money laundering or the activities of forensic laboratories.
(19) 公共の安全への脅威からの保護及びその脅威の抑止を含め、犯罪行為の防止、捜査、検知若しくは訴追又は刑罰の執行の目的のため、並びに、そのデータの自由な移動の目的のための所轄官庁による個人データの取扱いと関連する自然人の保護は、EU の特別の法的行為に服する。それゆえ、本規則は、それらの目的のための取扱行為に適用されない。ただし、本規則に基づく公的機関による個人データの取扱いは、それらの目的のために用いられるときは、EU のさらに特別の法律行為、すなわち、欧州議会及び理事会の指令(EU) 2016/680[7] によって規律される。加盟国は、それが EU 法の適用範囲内にある限り、それらの別の目的のための個人データの取扱いが本規則の適用範囲内にあるようにするため、指令(EU) 2016/680 の意味における所轄官庁に対し、

[7] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data and repealing Council Framework Decision 2008/977/JHA (see page 89 of this Official Journal).
犯罪行為の防止、捜査、探知若しくは訴追又は刑罰の執行のための所轄官庁による個人データの取扱いと関連する自然人の保護、及び、そのデータの自由な移動に関する、並びに、理事会枠組み決定 2008/977/JHA を廃止する 2016 年 4 月 27 日の欧州議会及び理事会の指令(EU) 2016/680（この官報の 89 頁参照）

公共の安全への脅威からの保護及びその脅威の防止を含め、犯罪行為の防止、捜査、検知若しくは訴追又は刑罰の執行の目的で行われる必要のない職務を委任できる。
本規則の適用範囲内にある目的のためのそれらの所轄官庁による個人データの取扱いに関して、加盟国は、本規則の規定の適用を調整するためのより特則的な条項を維持し、又は、それを導入できる。そのような条項は、それぞれの加盟国の国家体制上、国家組織上及び行政上の構造を考慮に入れた上で、それらの別の目的のための所轄官庁による個人データの取扱いについて、より詳細に特別の要件を定めることができる。民間組織による個人データの取扱いが本規則の適用範囲内にある場合、本規則は、公共の安全への脅威からの保護及びその脅威の防止を含め、公共の安全、犯罪行為の防止、捜査、検知若しくは訴追又は刑罰の執行を含む特別に重要な利益の保護のために、民主社会において必要であり、かつ、比例的な措置であるときは、加盟国が、特別の条件の下で、法律に基づき、一定の義務と権利を制限できることを定めなければならない。これは、例えば、反マネーロンダリングの枠組み又はフォレンジック調査機関の活動と関連するものである。

(20) While this Regulation applies, inter alia, to the activities of courts and other judicial authorities, Union or Member State law could specify the processing operations and processing procedures in relation to the processing of personal data by courts and other judicial authorities. The competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of the judiciary in the performance of its judicial tasks, including decision-making. It should be possible to entrust supervision of such data processing operations to specific bodies within the judicial system of the Member State, which should, in particular ensure compliance with the rules of this Regulation, enhance awareness among members of the judiciary of their obligations under this Regulation and handle complaints in relation to such data processing operations.
(20) 本規則が、特に、裁判所及びその他の司法機関の活動に対して適用されるのとは別に、EU 法又は加盟国の国内法は、裁判所及びその他の司法機関による個人データの取扱いと関連する取扱業務及び取扱手続を定めることができる。判決を含め、その司法上の職務の遂行における司法権の独立を保護するため、裁判所がその司法上の権能において行動する場合における個人データの取扱いに対しては、監督機関の職務権限が及ぶものとしてはならない。加盟国の司法制度内にある特別の組織に対してそのようなデータ取扱業務の監督を委任できるものとしなければならない。その組織は、特に、本規則の規定の遵守を確保し、司法機関の構成員の間に、本規則に基づく司法機関の義務の認識を拡大し、そして、そのようなデータ取扱業務と関連する不服申立てを取り扱わなければならない。

(21) This Regulation is without prejudice to the application of Directive 2000/31/EC of the European Parliament and of the Council [8], in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive. That Directive seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between Member States.
(21) 本規則は、欧州議会及び理事会の指令 2000/31/EC[8]の適用、特に、同指令の第 12 条ないし第 15 条に定める中間介在者であるサービスプロバイダの法的責任に関する法令の適用を妨げない。同指令は、加盟国間における情報社会サービスの自由な移動を確保することによって、域内市場の適正な機能に貢献することを求めるものである。

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

[8] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ L 178, 17.7.2000, p. 1).
域内市場における情報社会サービスの一定の法的側面特に電子商取引に関する欧州議会及び理事会の 2000 年 6 月 8 日の指令 2000/31/EC（電子商取引指令）（OJ L 178, 17.7.2000, p.1）

(22) EU 域内の管理者又は処理者の拠点の活動の過程における個人データの取扱いは、その取扱いそれ自体が EU 域内で行われたか否かにかかわらず、本規則に従って行われなければならない。拠点とは、安定的な仕組みを通じて行われる実効的かつ現実の活動の実施を意味する。そのような仕組みの法的形式、その支店又は法人格を有する子会社を通じているかは、この点に関する決定的要素とならない。

(23) In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment. In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union. Whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.
(23) 自然人が本規則に基づいて与えられる保護を妨げられないことを確保するために、EU 域内に拠点のない管理者又は処理者による EU 域内のデータ主体の個人データの取扱いは、その取扱行為が、支払いと関係するか否かにかかわらず、そのようなデータ主体に対する物品又はサービスの提供と関連する場合には、本規則に服さなければならない。EU 域内のデータ主体に対してそのような管理者又は処理者が物品又はサービスを提供しているか否かを判断するために、EU 域内の一又は複数の加盟国内のデータ主体に対してその管理者又は処理者がサービスを提供しようとする意図が明白かどうかを確認しなければならない。単に管理者、処理者又はその中間介在者の EU 域内の Web サイト、電子メールアドレス又はその他の連絡先にアクセスできるということ、又は、管理者が拠点とする第三国において一般的に用いられている言語が使用されているということだけでは、そのような意図を確認するためには不十分であるが、一又は複数の加盟国内で一般的に用いられている言語及び通貨を用いて当該別の言語による物品及びサービスの注文ができること、又は、EU 域内にいる消費者又は利用者に関する言及があることといったような要素は、その管理者が EU 域内のデータ主体に対して物品又はサービスの提供を想定していることを明白にしうるものである。

(24) The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union. In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.
(24) EU 域内に拠点のない管理者又は処理者による EU 域内のデータ主体の個人データの取扱いは、そのようなデータ主体の行動の監視と関連する場合においても、そのデータ主体の行動が EU 域内で行われるものである限り、本規則に服さなければならない。取扱行為がデータ主体の行動の監視と考えられうるか否かを判断するためには、自然人のプロファイリングを構成する個人データの取扱い技術が後に使用される可能性を含め、自然人がインターネット上で追跡されているかどうか、特に、データ主体に関連する判断をするため、又は、データ主体の個人的な嗜好、行動及び傾向を分析又は予測するために追跡されているかを確認しなければならない。

(25) Where Member State law applies by virtue of public international law, this Regulation should also apply to a controller not established in the Union, such as in a Member State's diplomatic mission or consular post.
(25)国際法の効力によって加盟国の国内法が適用される場合、EU 域内に拠点のない管理者、例えば加盟国の大

使館又は領事館などに対しても、本規則が適用されなければならない。

(26) The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.
(26) データ保護の基本原則は、識別された自然人又は識別可能な自然人に関する全ての情報に対して適用されなければならない。追加情報を使用しての利用によって自然人に属することを示しうる、仮名化を経た個人データは、識別可能な自然人に関する情報として考えられなければならない。ある自然人が識別可能であるかどうかを判断するためには、選別のような、自然人を直接又は間接に識別するために管理者又はそれ以外の者によって用いられる合理的な可能性のある全ての手段を考慮に入れなければならない。自然人を識別するために手段が用いられる合理的な可能性があるか否かを確認するためには、取扱いの時点において利用可能な技術及び技術の発展を考慮に入れた上で、識別のために要する費用及び時間量のような、全ての客観的な要素を考慮に入れなければならない。それゆえ、データ保護の基本原則は、匿名情報、すなわち、識別された自然人又は識別可能な自然人との関係をもたない情報、又は、データ主体を識別できないように匿名化された個人データに対しては、適用されない。本規則は、それゆえ、統計の目的又は調査研究の目的を含め、そのような匿名情報の取扱いに関するものではない。

(27) This Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons.
(27) 本規則は、死亡した者の個人データには適用されない。加盟国は、死亡した者の個人データの取扱いに関する規定を定めることができる。

(28) The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations. The explicit introduction of ‘pseudonymisation’ in this Regulation is not intended to preclude any other measures of data protection.
(28) 個人データに仮名化を適用することは、関係するデータ主体に対するリスクを低減させうるものであり、また、管理者及び処理者がそのデータ保護上の義務を遵守することを助けるものである。本規則における「仮名化」の明示的な導入は、データ保護のためのそれ以外の手段を排除することを意図するものではない。

(29) In order to create incentives to apply pseudonymisation when processing personal data, measures of pseudonymisation should, whilst allowing general analysis, be possible within the same controller when that controller has taken technical and organisational measures necessary to ensure, for the processing concerned, that this Regulation is implemented, and that additional information for attributing the personal data to a specific data subject is kept separately. The controller processing the personal data should indicate the authorised persons within the same controller.
(29) 個人データを取扱う際に仮名化を適用するインセンティブをつくり出すために、一般的な分析を認めることとは別に、関係する取扱いについて、本規則が実装されること、及び、特定のデータ主体に対して個人データを割り当てるための追加情報が別個に保管されることを確保するために必要となる技術上の措置及び組織上の措置を管理者が講じたときは、同一管理者内において、仮名化の手段を利用できるものとしなければならない。個人データを取扱う管理者は、同一管理者内で権限を与えられた者を表示しなければならない。

(30) Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.
(30) 自然人は、インターネットプロトコルアドレス、クッキー識別子、又は、無線識別タグのようなその他の識別子といったような、当該自然人のデバイス、アプリケーション、ツール及びプロトコルによって提供されるオンライン識別子と関連付けられうる。これは、特に、サーバによって受信されるユニーク識別子及びその他の情報と組み合わされるときは、自然人のプロファイルをつくり出し、そして、自然人を識別するために用いられうる痕跡を残しうるものである。

(31) Public authorities to which personal data are disclosed in accordance with a legal obligation for the exercise of their official mission, such as tax and customs authorities, financial investigation units, independent administrative authorities, or financial market authorities responsible for the regulation and supervision of securities markets should not be regarded as recipients if they receive personal data which are necessary to carry out a particular inquiry in the general interest, in accordance with Union or Member State law. The requests for disclosure sent by the public authorities should always be in writing, reasoned and occasional and should not concern the entirety of a filing system or lead to the interconnection of filing systems. The processing of personal data by those public authorities should comply with the applicable data-protection rules according to the purposes of the processing.
(31) 税務当局及び税関当局、金融情報部門、独立公的機関、又は、証券市場の規制及び監督の職責をもつ金融市場当局のような、それらの機関の公的な任務を実施すべき法的義務に従って個人データの開示を受ける公的機関は、それらの機関が、EU 法又は加盟国の国内法に従い、一般的な利益における特別の調査を行うために必要な個人データを取得する場合、個人データの取得者とはみなされない。そのような公的機関から送られるデータ開示要求は、常に、書面により、理由を付し、かつ、個別的なものでなければならず、かつ、ファイリングシステム全体にかかわるものであってはならず、かつ、ファイリングシステムへの相互接続となるものであってもならない。それらの公的機関による個人データの取扱いは、その取扱いの目的によって適用されるデータ保護法令を遵守するものでなければならない。

(32) Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.
(32) 同意は、電子的な手段による場合を含む書面による記述又は口述などにより、自己と関連する個人データの取扱いに対するデータ主体の合意の、自由に与えられ、特定され、事前に説明を受け、不明瞭ではない表示を構成する、明らかに肯定的な行為によって与えられるものとしなければならない。この同意は、インターネット Web サイトを訪問する際にボックスをチェックすること、情報社会サービスのための技術的な設定を選択すること、又は、この文脈において、自己の個人データについて提案された取扱いについてのデータ主体の承諾を明確に示す上記以外の陳述又は行為を含みうる。それゆえ、沈黙、予めチェック済みのボックス又は不作為は、同意を構成するものとしてはならない。同意は、同じ目的のために行われる全ての取扱活動を包摂しなければならない。取扱いが複数の目的をもつ場合、同意は、それらの全ての目的に対して与えられなければならない。データ主体の同意が電子的な手段による要求の後に与えられる場合、その要求は、明確であり、理解しやすく、かつ、提供されるサービスの利用を不必要に損なわないものでなければならない。

(33) It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.
(33) 科学研究の目的のための個人データの取扱いの目的をそのデータ収集の時点で完全に特定することは、しばしば、不可能なことである。それゆえ、データ主体は、科学研究のための広く認められた倫理基準が保たれている場合、一定の分野の科学研究に対して同意を与えることができる。データ主体は、予定されている目的が許す範囲内で、一定の分野の科学研究のみ、又は、研究プロジェクトの一部分のみに対して同意を与える機会をもつものとしなければならない。

(34) Genetic data should be defined as personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained.
(34) 遺伝子データは、自然人の、先天的な又は後天的な遺伝的特性に関する個人データとして定義される。それは、当の自然人から得られた生体サンプルの分析結果、特に、染色体、デオキシリボ核酸（DNA）又はリボ核酸（RNA）の分析の結果、又は、それらと同等の情報を得ることのできる他の要素の分析結果である。

(35) Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council [9] to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.
(35) 健康に関する個人データは、データ主体の健康状態と関係のあるデータであって、データ主体の過去、現在及び未来の身体状態又は精神状態に関する情報を明らかにする全てのデータを含む。このデータは、欧州議会及び理事会の指令 2011/24/EU [9]に定める医療サービスのための当該自然人の登録過程において、又は、その医療サービスの当該自然に対する提供の過程において収集されるその自然人に関する情報；医療上の目的で自然人をユニークに識別するために自然人に対して特別に割り当てられた番号、シンボル又は項目；遺伝子データ及び生化学的資料を含め、身体の一部又は身体組成物の試験若しくは検査から生じる情報；並びに、例えば、医師その他の医療専門職、病院、医療機器又は体外臨床検査のような当該情報の情報源の別を問わず、例えば、データ主体の疾病、障害、疾病リスク、病歴、診療治療、生理学的状態又は生物医学的状態を示す全ての情報を含む。

(36) The main establishment of a controller in the Union should be the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union, in which case that other establishment should be considered to be the main establishment. The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes and means of processing through

[9] 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).
国境を越える医療における患者の権利の適用に関する欧州議会及び理事会の 2011 年 3 月 9 日の指令 2011/24/EU（OJ L 88, 4.4.2011, p.45）

stable arrangements. That criterion should not depend on whether the processing of personal data is carried out at that location. The presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute a main establishment and are therefore not determining criteria for a main establishment. The main establishment of the processor should be the place of its central administration in the Union or, if it has no central administration in the Union, the place where the main processing activities take place in the Union. In cases involving both the controller and the processor, the competent lead supervisory authority should remain the supervisory authority of the Member State where the controller has its main establishment, but the supervisory authority of the processor should be considered to be a supervisory authority concerned and that supervisory authority should participate in the cooperation procedure provided for by this Regulation. In any case, the supervisory authorities of the Member State or Member States where the processor has one or more establishments should not be considered to be supervisory authorities concerned where the draft decision concerns only the controller. Where the processing is carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered to be the main establishment of the group of undertakings, except where the purposes and means of processing are determined by another undertaking.
(36) EU 域内における管理者の主たる拠点は、EU 域内における管理者の統括管理部門の所在地としなければならない。ただし、個人データの取扱いの目的及び方法の決定が EU 域内の管理者の別の拠点において行われる場合を除く。この場合、当該別の拠点が主たる拠点とみなされる。EU 域内における管理者の主たる拠点は、客観的な基準に従って判断されなければならず、また、安定的な仕組みを通じて、取扱いの目的及び方法に関する主要な判断事項に関する決定をするという管理行為が実効的かつ現実になされていることを示すものでなければならない。その基準は、個人データの取扱いが当該の場所で行われているか否かには依拠しない。個人データの取扱い又は取扱活動のための技術的手段及び技術が存在すること及びそれが利用されていることは、それ自体としては、主たる拠点を構成するものではなく、それゆえ、そのことは、主たる拠点についての決定的基準とならない。処理者の主たる拠点は、EU 域内における中枢機関の所在地とし、又は、EU 域内に統括管理部門が存在しない場合は、EU 域内において主要な取扱活動が行われる場所とすべきである。管理者と処理者の両者が関与するケースでは、管轄する主監督機関は管理者が主たる拠点をもつ加盟国の監督機関であり続けるが、処理者の監督機関は、関係監督機関とみなされるべきであり、また、当該監督機関は、本規則によって定められる協力手続に参加するべきである。いずれにせよ、処理者が一又は複数の拠点をもつ加盟国の監督機関は、決定案が管理者にのみ関係するものである場合には、関係監督機関とはみなされない。取扱いが企業グループによって行われる場合、取扱いの目的及び方法が別の企業によって決定される場合を除き、支配権をもつ企業の主たる拠点がその企業グループの主たる拠点とみなされる。

(37) A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exert a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented. An undertaking which controls the processing of personal data in undertakings affiliated to it should be regarded, together with those undertakings, as a group of undertakings.
(37) 企業グループは、支配権をもつ企業とその企業による支配を受ける企業とを包含ものであり、支配権をもつ企業は、例えば、所有関係、資金関係若しくは規律するルールよって、若しくは、個人データ保護のルールを実施する権限によって、他の企業に対して支配的な影響力を及ぼすことのできる企業である。関係する企業の個人データの取扱いを管理する企業は、それらの企業と共に、企業グループとみなされる。

(38) Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.
(38) 子どもは、個人データの取扱いと関連するリスク、結果及び関係する保護措置、並びに、自らの権利につ

いて十分に認識できないかもしれないため、その個人データに関して特別の保護を享受する。特に、マーケティングの目的、その子どもに関するパーソナリティ若しくは個人プロファイルの作成の目的での子供についての個人データの使用、及び子どもに対して直接に提示されるサービスを利用する際の子どもの個人データの収集に対して、そのような特別の保護が適用されなければならない。子どもに対して直接に提供される予防的サービスサービス又はカウンセリングサービスの文脈においては、親権を有する者の同意を要しない。

(39) Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing.
(39) いかなる個人データの取扱いも適法かつ公正でなければならない。自然人に関する個人データが収集され、利用され、調査され、又は、それら以外の取扱いをされていること、及び、どの範囲の個人データが取扱われており、又は、取扱われることになるのかが、当該自然人に対して明らかにされなければならない。透明性の原則は、それらの個人データの取扱いと関連する情報及びコミュニケーションに容易にアクセスできること及び容易に理解できること、また、明確かつ平易な文言が用いられることを求める。この基本原則は、特に、データ主体に対する管理者の識別名及び取扱いの目的の情報、並びに、関係する自然人に関する公正かつ透明性のある取扱いを確保し、そして、取扱われている自然人に関する個人データの確認及びコミュニケーションを得る当該自然人の権利を確保するためのさらなる情報と関係している。自然人は、個人データの取扱いと関連するリスク、ルール、保護措置及び権利、並びに、その取扱いと関連する自身の権利をどのように行使するかについて、知らされなければならない。特に、個人データを取扱うための特定の目的は、その個人データの収集の時点において、明確なものであり、正当なものであり、かつ、確定されたものでなければならない。個人データは、それが取扱われる目的のために十分であり、関連性があり、それに必要な範囲に限定されるものでなければならない。このことは、特に、個人データが記録保存される期間が厳密に最小限に限られることを確保することを求める。個人データは、その取扱いの目的が他の手段によっては合理的に満たされない場合においてのみ、取扱われるものとしなければならない。個人データが必要な範囲を超えて保存されないことを確保するために、消去又は定期的な見直しのための期限が管理者によって設けられなければならない。不正確な個人データが訂正又は削除されることを確保するための全ての合理的な手段が講じられなければならない。個人データは、個人データ及び取扱いに用いられる装置に対する無権限のアクセス又はその無権限使用の防止に関するものを含め、個人データの適切な安全性及び機密性を確保する態様で、取扱われればならない。

(40) In order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation, including the necessity for compliance with the legal obligation to which the controller is subject or the necessity for the performance of a contract to which the data subject is party or in order to take steps at the

request of the data subject prior to entering into a contract.
(40) 取扱いが適法であるものとするために、個人データは、関係するデータ主体の同意に基づいて、又は、管理者が服すべき法的義務遵守のための必要性、若しくは、データ主体が当事者となっている契約の履行のための必要性、又は、契約を締結する前のデータ主体による要求により手段を講ずるための場合を含め、データ主体の同意以外の、本規則の中で、又は、本規則に定める EU 法若しくは加盟国の国内法の中で法律によって定められるいくつかの正当化根拠に基づいて、取扱われなければならない。

(41) Where this Regulation refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned. However, such a legal basis or legislative measure should be clear and precise and its application should be foreseeable to persons subject to it, in accordance with the case-law of the Court of Justice of the European Union (the 'Court of Justice') and the European Court of Human Rights.
(41) 本規則が法的根拠又は立法措置に言及する場合、それは、関係加盟国の憲法秩序による要件を妨げることなく、議会によって採択される立法行為を必ずしも要求するものではない。ただし、そのような法的根拠又は立法措置は、欧州司法裁判所（以下「欧州司法裁判所」という。）及び欧州人権裁判所の判例法に従い、明確かつ正確であることを要し、かつ、その適用は、それに服する者にとって予測可能なものでなければならない。

(42) Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. In accordance with Council Directive 93/13/EEC [10] a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.
(42) 取扱いがデータ主体の同意に基づく場合、管理者は、そのデータ主体がその取扱業務に対して同意を与えたということを証明できるようにしなければならない。特に、他の事項に関して書面上の宣言をする状況においては、保護措置は、同意が与えられることになるという事実及びその同意が与えられる範囲についてデータ主体が認識することを確保しなければならない。理事会指令 93/13/EEC [10]に従い、管理者によって事前に書式化された同意の宣言は、理解しやすく、容易にアクセスできる方式により、明確かつ平易な文言を用いて示されなければならず、かつ、不公正な条件を含むものであってはならない。通知される同意に関し、そのデータ主体は、少なくとも、管理者の身元、及び、その個人データについて予定されている取扱いの目的を認識していなければならない。データ主体が真の又は自由の選択でない場合、又は、不利益を受けずにその同意を拒否又は撤回できない場合、その同意は、自由に与えられたものとはみなされない。

(43) In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.
(43) 同意が自由に与えられることを確保するために、データ主体と管理者との間に明確な不均衡が存在する特別な場合、特に、管理者が公的機関である場合で、それゆえに、当該状況の全体からみて、同意が自由に与えられる可能性が低いようなときには、その同意は、個人データを取扱うための有効な法的根拠を提供するもの

[10] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (OJ L 95, 21.4.1993, p. 29).
消費者契約における不公正な契約条件に関する 1993 年 4 月 5 日の理事会指令 93/13/EEC（OJ L 95, 21.4.1993, p.29）

とはならない。個々の場合に個別に同意することが適切であるにもかかわらず、異なる個人データ取扱業務毎に分けて同意を与えることが認められない場合、又は、サービス契約の履行のためにそのような同意を必要としないのにもかかわらず、サービスの提供の場合を含め契約の履行が同意を必要としている場合、そのような同意は、自由に与えられたものではないと推定される。

(44) Processing should be lawful where it is necessary in the context of a contract or the intention to enter into a contract.
(44) 契約の過程において必要となる場合、又は、契約の締結に入る意図の場合、その取扱いは適法である。

(45) Where processing is carried out in accordance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, the processing should have a basis in Union or Member State law. This Regulation does not require a specific law for each individual processing. A law as a basis for several processing operations based on a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority may be sufficient. It should also be for Union or Member State law to determine the purpose of processing. Furthermore, that law could specify the general conditions of this Regulation governing the lawfulness of personal data processing, establish specifications for determining the controller, the type of personal data which are subject to the processing, the data subjects concerned, the entities to which the personal data may be disclosed, the purpose limitations, the storage period and other measures to ensure lawful and fair processing. It should also be for Union or Member State law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or, where it is in the public interest to do so, including for health purposes such as public health and social protection and the management of health care services, by private law, such as a professional association.
(45) 管理者が服すべき法的義務に従って取扱いが行われる場合、又は、公共の利益において、若しくは、公的な権限の行使において行われる職務の遂行のために取扱いが必要となる場合、その取扱いは、EU 法又は加盟国の国内法に根拠をもつものとしなければならない。本規則は、個々の取扱いに関する特別の法律を要求しない。管理者が服すべき法的義務に基づくいくつかの取扱業務のための根拠として、又は、公共の利益において、若しくは、公的な権限の行使において行われる職務の遂行のために取扱いが必要となる場合の根拠として、法律は、十分なものでありうる。その取扱いの目的を決定するのも EU 法又は加盟国の国内法でなければならない。また、その法律は、個人データの取扱いの適法性を規律する本規則の一般的な要件の細則を定め、管理者、取扱いの対象となる個人データの種類、関係するデータ主体、個人データの開示を受けることができる組織、目的の制限、記録保存期間を決定するための詳細を定め、並びに、これ以外の適法かつ公正な取扱いを確保するための措置を定めることができる。EU 法又は加盟国の国内法は、公共の利益において、若しくは、公的な権限の行使において行われる職務を遂行する管理者が、公的機関又はそれ以外の公法によって規律される自然人若しくは法人でなければならないかどうか、又は、公衆衛生や社会保障のような医療上の目的の場合並びに専門職の団体のような私法による公衆衛生サービスの管理の場合を含め、どのような取扱いが公共の利益によるものとなるかについても定めなければならない。

(46) The processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters.
(46) 個人データの取扱いは、データ主体の生命又は他の自然人の生命にとって本質的な利益を保護するために必要である場合、適法なものとみなされる。他の自然人の生命に関する利益を根拠とする個人データの取扱いは、原則として、その取扱いが、他の法的根拠に基づきえないことが明白である場合においてのみ、行われるものとしなければならない。例えば、感染症及びその感染域の監視を含め、人道上の目的のために取扱いが必

要となる場合、又は、人道上の緊急性のある状況下にある場合、特に、自然災害や人為的な災害の状況下にある場合のように、いくつかの種類の取扱いでは、公共の利益及びデータ主体の生命に関する利益の両者が重要な根拠となりうる。

(47) The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing. Given that it is for the legislator to provide by law for the legal basis for public authorities to process personal data, that legal basis should not apply to the processing by public authorities in the performance of their tasks. The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.
(47) 個人データの開示を受けうる管理者の正当な利益を含め、管理者又は第三者の正当な利益は、データ主体と管理者との関係に基づくデータ主体の合理的な期待を考慮に入れた上で、データ主体の利益又は基本的な権利及び自由を覆すものとならない場合に、取扱いのための法的根拠を提供しうる。そのような正当な利益は、例えば、データ主体が管理者のサービスの顧客である場合や管理者からサービスの提供を受けている場合のような状況において、データ主体と管理者との間に妥当で適切な関係がある場合には、存在しうる。いずれにせよ、個人データの収集の時点において、及び、その過程において、当該目的のために取扱いが行われることをデータ主体が合理的に期待できるか否かを含め、正当な利益の存在に関しては、注意深い評価を要するであろう。データ主体が合理的にさらなる取扱いを予期しない状況下で個人データが取扱われる場合、特に、データ主体の利益及び基本的な権利は、データ管理者の利益よりも優先しうる。公的機関に関して個人データを取扱うための法的根拠を法律によって定めるのが立法者であることに鑑み、当該法的根拠は、公的機関がその職務の遂行において行う取扱いに適用してはならない。不正行為の防止の目的のために厳密に必要性のある個人データの取扱いもまた、関係するデータ管理者の正当な利益を構成する。ダイレクトマーケティングのための個人データの取扱いは、正当な利益のために行われるものとみなされうる。

(48) Controllers that are part of a group of undertakings or institutions affiliated to a central body may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data. The general principles for the transfer of personal data, within a group of undertakings, to an undertaking located in a third country remain unaffected.
(48) 企業グループの一員又は統括企業と提携する組織の一員である管理者は、顧客又は従業員の個人データの取扱いを含め、内部的な業務管理の目的のために、その企業グループ内において個人データを移転することについて、正当な利益をもちうる。企業グループ内での第三国に所在する企業に対する個人データの移転についての一般原則は、影響を受けない。

(49) The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and

services, constitutes a legitimate interest of the data controller concerned. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.
(49) ネットワーク及び情報の安全性を確保する目的のために厳密に必要性であり、かつ、比例的な範囲内で行われる個人データの取扱い、例えば、保存される個人データ若しくは送信される個人データの可用性、真正性、完全性及び機密性を阻害し、また、公的機関、コンピュータ緊急対応チーム（CERT）、コンピュータセキュリティインシデント対応チーム（CSIRT）、電子通信ネットワークのプロバイダ及び電子通信サービスのプロバイダ、並びに、セキュリティ技術及びセキュリティサービスの提供者によって、そのネットワーク及びシステムを介して提供され又はアクセス可能なものとされている関連サービスの安全性を阻害する事故、又は、違法な行為若しくは悪意ある行為に対して、所与の機密性のレベルにおいて対抗するためのネットワークシステム又は情報システムの能力を確保することは、関係するデータ管理者の正当な利益を構成する。これには、例えば、電子通信ネットワークへの無権限アクセス及び悪意あるコード配布を防止すること、並びに、「サービス拒否」攻撃やコンピュータ及び電子通信システムの破壊行為を阻止することが含まれうる。

(50) The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required. If the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Union or Member State law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. The legal basis provided by Union or Member State law for the processing of personal data may also provide a legal basis for further processing. In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, inter alia: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations.
Where the data subject has given consent or the processing is based on Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard, in particular, important objectives of general public interest, the controller should be allowed to further process the personal data irrespective of the compatibility of the purposes. In any case, the application of the principles set out in this Regulation and in particular the information of the data subject on those other purposes and on his or her rights including the right to object, should be ensured. Indicating possible criminal acts or threats to public security by the controller and transmitting the relevant personal data in individual cases or in several cases relating to the same criminal act or threats to public security to a competent authority should be regarded as being in the legitimate interest pursued by the controller. However, such transmission in the legitimate interest of the controller or further processing of personal data should be prohibited if the processing is not compatible with a legal, professional or other binding obligation of secrecy.
(50) 個人データが収集された当初の目的とは異なる目的のための個人データの取扱いは、その取扱いが、その個人データが収集された当初の目的と適合する場合に限り、認められる。そのような場合、その個人データの収集を認めた法的根拠とは異なる法的根拠は要求されない。公共の利益において又は管理者に与えられた公的な権限の行使において行われる職務の遂行のためにその取扱いが必要となる場合、EU 法若しくは加盟国の国内法は、その追加的取扱いが、適合的かつ適法なものとみなされるべき場合に関する職務及び目的を定め、特定しうる。公共の利益における保管の目的、科学的研究若しくは歴史的研究の目的又は統計の目的のための追加的取扱いは、適合的で適法な取扱業務とみなされる。個人データの取扱いのために EU 法又は加盟国の国内法によって定められる法的根拠は、追加的取扱いのための法的根拠についても提供しうる。追加的取扱いの目

的が、その個人データが収集された当初の目的と適合するか否かを確認するために、管理者は、当初の取扱いの適法性のための全ての要件を満たした後、特に：当初の目的と予定されている追加的取扱いの目的との間の関連性；個人データが取得された経緯、特に、個人データのさらなる利用に関するデータ主体と管理者との間の関係に基づくデータ主体の合理的な期待；個人データの性質；意図する追加的取扱いのデータ主体への結果；並びに、当初の取扱業務及び予意図する追加的取扱業務の両方についての適切な保護措置の存在、を考慮に入れなければならない。

データ主体が同意を与えている場合、又は、その取扱いが、特に、一般的な公共の利益の重要な目的を守るために民主主義の社会において必要かつ比例的な手段を構成するEU法若しくは加盟国の国内法に基づくものである場合、管理者は、その目的の適合性の有無にかかわらず、個人データを追加的に取扱うことが認められなければならない。いずれの場合においても、本規則に定める基本原則が適用されること、並びに、特に、当該別の目的、及び、異議を述べる権利を含めたデータ主体の権利に関し、データ主体に対する情報提供が確保されなければならない。犯罪行為又は公共の安全に対する脅威がありうることについて管理者が指摘すること、及び、同じ犯罪行為又は公共の安全に対する脅威と関連する個々の事案若しくはいくつかの事案において、所轄官庁に対して関連する個人データを送付することは、管理者により正当な利益において行われるものとみなされる。ただし、そのような管理者の正当な利益における個人データの移転又は追加的取扱いは、その取扱いが、法律上の守秘義務、職務上の守秘義務又はそれ以外の拘束力のある守秘義務に適合しないときは、禁止されなければならない。

(51) Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data should include personal data revealing racial or ethnic origin, whereby the use of the term 'racial origin' in this Regulation does not imply an acceptance by the Union of theories which attempt to determine the existence of separate human races. The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person. Such personal data should not be processed, unless processing is allowed in specific cases set out in this Regulation, taking into account that Member States law may lay down specific provisions on data protection in order to adapt the application of the rules of this Regulation for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. In addition to the specific requirements for such processing, the general principles and other rules of this Regulation should apply, in particular as regards the conditions for lawful processing. Derogations from the general prohibition for processing such special categories of personal data should be explicitly provided, inter alia, where the data subject gives his or her explicit consent or in respect of specific needs in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.
(51) その性質上基本的な権利及び自由との関係において特にセンシティブな個人データは、その取扱いの過程が基本的な権利及び自由に対する深刻なリスクをつくり出しうるものであるため、特別の保護を受ける。それらの個人データは、人種的又は民族的な出自を明らかにする個人データを含むが、本規則の中における「人種的な出自」という用語の使用は、それによって、異なる人種の存在を決定しようとする思想をEUが受容することを意味するものではない。写真の取扱いは、特別な種類の個人データの取扱いであると即断してはならない。なぜなら、自然人を一意に識別又は認証をすることができる特別な技術的手段を用いて取扱われる場合においてのみ生体データに含まれるからである。法律上の義務を遵守するため、又は、公共の利益において若しくは管理者に与えられた公的な権限の行使において行われる職務の遂行のために、本規則の規定の適用を採択するためのデータ保護に関する特別な条項を加盟国の国内法が定めることができることを考慮に入れた上で、本規則に定める特別な場合に該当する場合において取扱いが許容される場合を除き、そのような個人データを取扱ってはならない。そのような取扱いに関する特別の要件に加え、特に、適法な取扱いのための要件に関し、本規則の一般的な基本原則及びその他の規定が適用される。そのような特別な種類の個人データの取扱いの一般的な禁止の例外は、特に、データ主体が明示の同意を与える場合、又は、その特別の必要性に関して、特に、基本的な自由の行使を許容することを目的とする一定の団体若しくは協会による正当な活動の過程において

その取扱いが行われる場合において、明確に定められなければならない。

(52) Derogating from the prohibition on processing special categories of personal data should also be allowed when provided for in Union or Member State law and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where it is in the public interest to do so, in particular processing personal data in the field of employment law, social protection law including pensions and for health security, monitoring and alert purposes, the prevention or control of communicable diseases and other serious threats to health. Such a derogation may be made for health purposes, including public health and the management of health-care services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. A derogation should also allow the processing of such personal data where necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure.
(52) 公共の利益において行われる場合であり、特に、労働法の分野、年金及び医療保険を含む社会保護法の分野における個人データの取扱い、伝染病及びその他の健康に対する重大な脅威の防止又は管理のための監視及び警戒の目的の場合において、個人データ及びその他の基本的な権利を保護するために、EU 法又は加盟国の国内法の中に定められており、かつ、適切な保護措置に従うものであれば、特別な種類の個人データの取扱いの禁止の例外も認められる。公衆衛生及び医療サービスの管理を含め、医療の目的のために、特に健康保険制度における給付及びサービスの提供の請求を取扱うために用いられる手続の品質及び費用対効果を確保するため、又は、公共の利益における保管の目的、科学的研究及び歴史的研究の目的並びに統計の目的のために、そのような例外を設けることができる。裁判所の訴訟手続、行政上の手続及び裁判外の手続のいずれにおいても、訴えの提起及び攻撃防御のために必要な場合には、例外としてそのような個人データの取扱いを許容する。

(53) Special categories of personal data which merit higher protection should be processed for health-related purposes only where necessary to achieve those purposes for the benefit of natural persons and society as a whole, in particular in the context of the management of health or social care services and systems, including processing by the management and central national health authorities of such data for the purpose of quality control, management information and the general national and local supervision of the health or social care system, and ensuring continuity of health or social care and cross-border healthcare or health security, monitoring and alert purposes, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, based on Union or Member State law which has to meet an objective of public interest, as well as for studies conducted in the public interest in the area of public health. Therefore, this Regulation should provide for harmonised conditions for the processing of special categories of personal data concerning health, in respect of specific needs, in particular where the processing of such data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy. Union or Member State law should provide for specific and suitable measures so as to protect the fundamental rights and the personal data of natural persons. Member States should be allowed to maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health. However, this should not hamper the free flow of personal data within the Union when those conditions apply to cross-border processing of such data.
(53) より高い保護を享受する特別な種類の個人データは、自然人及び社会全体の利益となる目的を達成するために必要となる場合に限り医療と関連する目的のために取扱われるものとしなければならない。特に、医療と社会福祉の提供及び制度の管理の過程における取扱い、特別な種類これには、公共の利益の目的と適合すべき EU 法又は加盟国の国内法に基づく、医療制度及び社会福祉制度の品質管理、情報管理及び国家的若しくは地域的な一般的監督の目的、及び、医療及び社会福祉並びに国境を越える医療又は健康保険の継続性を確保する目的、監視又は警告の目的、又は、公共の利益における保管の目的、科学的研究若しくは歴史的研究の目的又は統計の目的、並びに、公衆衛生の領域における公共の利益において行われる研究の目的のための、医療管理機関及び国家の中央医療公的組織によるデータの取扱いが含まれる。それゆえ、本規則は、特別の必要性に関し、特に、職務上の守秘義務という法的義務に服する者によって健康と関係する一定の目的のためにそのような個人データの取扱いが行われる場合に関し、健康と関係する特別な種類の個人データの取扱いのための整合

性のとれた要件を定めなければならない。EU 法又は加盟国の国内法は、自然人の基本的な権利及び個人データを保護するための特別の適切な措置を定めなければならない。加盟国は、遺伝子データ、生体データ又は健康に関するデータの取扱いに関し、その制限を含め、追加的な条件を維持又は導入することが認められなければならない。ただし、その条件がそのようなデータの国境を越える取扱いに適用される場合、その条件は、EU 域内における個人データの自由な流通を阻害してはならない。

(54) The processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject. Such processing should be subject to suitable and specific measures so as to protect the rights and freedoms of natural persons. In that context, 'public health' should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council [11], namely all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. Such processing of data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers or insurance and banking companies.
(54) 特別な種類の個人データの取扱いは、データ主体の同意なしに、公衆衛生の分野における公共の利益を理由として、必要となることがある。そのような取扱いは、自然人の権利及び自由を保護するための適切かつ具体的な措置に服するものでなければならない。この文脈において、「公衆衛生」とは、欧州議会及び理事会の規則 No 1338/2008[11]に定義されているように、すなわち、健康に関する全ての要素、換言すると、健康状態のこととして解釈されなければならない。それは、疾病率及び障害、健康状態に影響を与える素因、医療の必要性、医療に割り当てられる資源、医療の提供及び医療へのユニバーサルアクセス、並びに、医療の支出及び資金手当、そして、死亡原因を含む。そのような公共の利益を理由とする医療と関連する個人データの取扱いは、使用者、保険会社及び金融機関のような第三者によって別の目的のために個人データが取扱われる結果をもたらしてはならない。

(55) Moreover, the processing of personal data by official authorities for the purpose of achieving the aims, laid down by constitutional law or by international public law, of officially recognised religious associations, is carried out on grounds of public interest.
(55) また、憲法又は国際法によって定められている諸目的を達成する目的のために、公的機関による、公に認められている宗教団体の個人データの取扱いは、公共の利益を根拠として行われるものである。

(56) Where in the course of electoral activities, the operation of the democratic system in a Member State requires that political parties compile personal data on people's political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established.
(56) 選挙活動の過程において、加盟国における民主制度の運営のために、政党が人々の政治的意見に関する個人データを集約する必要がある場合、そのようなデータ取扱いは、適切な保護措置が設けられることを条件として、公共の利益を理由として認められうる。

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

---

[11] Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work (OJ L 354, 31.12.2008, p. 70).
公衆衛生並びに労働における健康及び安全上の欧州共同体の統計に関する欧州議会及び理事会の規則(EC) No 1338/2008（OJ L 354, 31.12.2008, p.70）

(57) 管理者によって取扱われる個人データが管理者による自然人の識別を許容しないものである場合、そのデータ管理者は、本規則の条項を遵守するという目的のみのために、データ主体を識別するための付加的な情報を入手することを義務付けられない。ただし、その管理者は、データ主体から自己の権利の行使をサポートするために提供される追加的な情報の取得を拒むことができない。識別には、例えば、データ管理者によって提供されるオンラインサービスにログインするためにデータ管理者から提供され、データ主体によって用いられる同一の認証情報のような認証手段を介するデータ主体のデジタル識別が含まれなければならない。

(58) The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used. Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising. Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.
(58) 透明性の原則は、公衆又はデータ主体に伝達される情報が、明解であり、容易にアクセスでき、かつ、容易に理解できるものであること、そして、明確かつ平易な文言、加えて、適切な場合には、視覚化技術が用いられていることを求める。そのような情報は、例えば、Web サイトを介して公衆に伝達される場合には、電子的な方式によって提供されうる。オンライン宣伝広告の場合のように、関与者の増加及び実務上の技術的な複雑さによって、自己の個人データが収集されるのかどうか、誰によって、何の目的のために収集されるのかをデータ主体が認識し、理解することを困難にされてしまっているような状況下においては、この原則は、特に関連性をもつものである。子どもが特別の保護を享受することに鑑み、取扱いが子ども向けのものであるときは、いかなる情報及び連絡も、子どもが容易に理解することのできるような明確かつ平易な文言によるものでなければならない。

(59) Modalities should be provided for facilitating the exercise of the data subject's rights under this Regulation, including mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and the exercise of the right to object. The controller should also provide means for requests to be made electronically, especially where personal data are processed by electronic means. The controller should be obliged to respond to requests from the data subject without undue delay and at the latest within one month and to give reasons where the controller does not intend to comply with any such requests.
(59) 本規則に基づくデータ主体の権利の行使を容易なものとするため、様式が定められなければならない。これには、特に、適用可能な場合は、個人データに対するアクセス及び個人データの訂正又は消去を無償で受けること、また、異議を述べる権利を行使することを要求するための仕組みが含まれる。特に電子的な方法で個人データが取扱われる場合、管理者は、電子的に要求するための方法も提供しなければならない。管理者には、不当な遅滞なく、遅くとも 1 か月以内に、データ主体からの要求に対応することこと、また、管理者がその要求に応ずるつもりがない場合には、その理由を提供することが義務付けられなければならない。

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

(60) 公正かつ透明性のある取扱いの原則は、その取扱業務の存在及びその目的について、データ主体が情報の提供を受けることを求める。管理者は、データ主体に対し、その個人データが取扱われる具体的な状況及びその取扱い過程を考慮に入れた上で、公正かつ透明性のある取扱いを確保するために必要な情報を別に提供しなければならない。さらに、データ主体は、プロファイリングの存在及びそのようなプロファイリングから生ずる結果についても情報の提供を受けるものとしなければならない。個人データがデータ主体から収集される場合、そのデータ主体は、自身がその個人データの提供を義務付けられているのか否かについて、及び、データ主体がそのデータを提供しない場合に生ずる結果についても情報の提供を受けるものとしなければならない。その情報は、容易に視認することができ、分かりやすく、明確に理解することのできる態様で、予定されている取扱いの意味のある概要を示すための標準的なアイコンと組み合わせて提供することができる。そのアイコンが電子的に表示される場合、それらは、機械可読性のあるものでなければならない。

(61) The information in relation to the processing of personal data relating to the data subject should be given to him or her at the time of collection from the data subject, or, where the personal data are obtained from another source, within a reasonable period, depending on the circumstances of the case. Where personal data can be legitimately disclosed to another recipient, the data subject should be informed when the personal data are first disclosed to the recipient. Where the controller intends to process the personal data for a purpose other than that for which they were collected, the controller should provide the data subject prior to that further processing with information on that other purpose and other necessary information. Where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided.
(61) データ主体に関する個人データの取扱いに関係する情報は、データ主体からの収集の時点において、又は、個人データが他の情報源から取得される場合には、事案の状況に応じて合理的な期間内に、当該データ主体に対して与えられなければならない。個人データが別の取得者に対して正当に開示されうる場合、そのデータ主体は、その個人データがその取得者に対して最初に開示される時に通知を受けるものとしなければならない。個人データが収集された目的とは別の目的のために管理者がその個人データを取扱いしようとする場合、その管理者は、別の目的による追加的取扱いの開始前に、そのデータ主体に対し、当該別の目的に関する情報及びその他の必要な情報を提供しなければならない。様々な情報源が用いられたために、データ主体に対してその個人データの入手元を示すことができない場合には、一般的な情報が提供されなければならない。

(62) However, it is not necessary to impose the obligation to provide information where the data subject already possesses the information, where the recording or disclosure of the personal data is expressly laid down by law or where the provision of information to the data subject proves to be impossible or would involve a disproportionate effort. The latter could in particular be the case where processing is carried out for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. In that regard, the number of data subjects, the age of the data and any appropriate safeguards adopted should be taken into consideration.
(62) ただし、データ主体が既にその情報を保有している場合、その個人データの記録若しくは開示が法律によって明確に定められている場合、又は、データ主体に対する情報の提供が明らかに不可能であるか、若しくは、過大な負担を生じさせるような場合、情報を提供すべき義務を課す必要はない。特に、公共の利益における保管の目的、科学的研究若しくは歴史的研究の目的又は統計の目的のために取扱いが行われる場合、データ主体に対する情報の提供が明らかに不可能であるか、若しくは、過大な負担を生じさせるような場合に該当しうる。この点に関し、データ主体の人数、データの経過年数及び導入されている適切な保護措置が考慮に入れられなければならない。

(63) A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing. This includes the right for data subjects to have access to data concerning their health, for example the data in their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided. Every data subject should therefore have the right to know and obtain communication in particular

with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing. Where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data. That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject. Where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates.
(63) データ主体は、当該データ主体に関して収集された個人データにアクセスする権利をもち、そして、その取扱いの適法性を意識し、それを検証するために、容易に、かつ、合理的な間隔で、その権利を行使する権利を有するものとしなければならない。この権利は、データ主体の健康に関するデータ、例えば、疾病の診断、検査結果、治療担当医師により行われた評価並びに提供された治療行為若しくは治療介入のような情報を含むデータ主体についての医療記録中にあるデータへアクセスするデータ主体の権利を含む。それゆえ、全てのデータ主体は、特に、その個人データが取扱われる目的、可能な場合には、その個人データが取扱われる期間、その個人データの取得者、自動的な個人データの取扱いの中に含まれている論理、並びに、少なくともプロファイリングに基づく場合、そのような取扱いの結果として発生しうる事態に関し、知る権利及び連絡を受ける権利を有するものとしなければならない。可能な場合、管理者は、データ主体に対して当該データ主体の個人データへの直接のアクセスを提供しうる安全なシステムへのリモートアクセスを提供できるようにしなければならない。その権利は、営業秘密又は知的財産及び特にソフトウェアの著作権を含め、他者の権利又は自由に不利な影響を与えてはならない。ただし、これらの考慮は、データ主体に対して全ての情報を提供することの拒絶となるものであってはならない。管理者がデータ主体に関する情報を大規模に取扱う場合、その管理者は、その情報が提供される前に、その要求と関連する情報又は取扱行為をデータ主体が特定するように要求することができるものとしなければならない。

(64) The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests.
(64) 管理者は、特に、オンラインサービス及びオンライン認証の過程において、アクセスを要求するデータ主体の身元を確認するための全ての合理的な手段を用いなければならない。管理者は、ありうる要求に対応するという目的のみのために個人データを保持してはならない。

(65) A data subject should have the right to have personal data concerning him or her rectified and a ‘right to be forgotten’ where the retention of such data infringes this Regulation or Union or Member State law to which the controller is subject. In particular, a data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation. That right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child. However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims.
(65)あるデータを保持することが、管理者が服すべき本規則又は EU 法若しくは加盟国の国内法の違反行為となる場合、データ主体は、当該データ主体に関する個人データを訂正させる権利及び「忘れられる権利」をも

つものとしなければならない。特に、データ主体は、当該個人データを収集する若しくはその他の取扱いをする目的との関連においてその個人データが必要なくなった場合、データ主体が同意を撤回した場合、若しくは、自己に関する個人データの取扱いに対して異議を述べる場合、又は、データ主体の個人データの取扱いが本規則を何ら遵守するものではない場合において、当該個人データの個人データを消去させ、取扱われないようにさせる権利を有するものとしなければならない。その権利は、特に、データ主体が、子どもの時に、その取扱いに含まれるリスクについて完全に理解しないまま自身の同意を与えたけれども、後になって、そのような個人データの削除、特にインターネット上のデータの削除を望むようになった場合において関連性がある。データ主体は、当該データ主体が既に子どもではないという事実とは無関係に、その権利を行使することができるものとしなければならない。ただし、表現及び情報伝達の自由の権利の行使のために必要な場合、法律上の義務を遵守するために必要な場合、公衆衛生の領域における公共の利益を法的根拠として、公共の利益において、又は、管理者に与えられた公的な権限の行使において行われる職務の遂行のために必要な場合、公共の利益における保管の目的、科学的研究若しくは歴史的研究の目的又は統計の目的のために必要な場合、又は、訴訟の提起若しくは攻撃防御のために必要がある場合には、そのためにさらに個人データを保持することを適法としなければならない。

(66) To strengthen the right to be forgotten in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform the controllers which are processing such personal data to erase any links to, or copies or replications of those personal data. In doing so, that controller should take reasonable steps, taking into account available technology and the means available to the controller, including technical measures, to inform the controllers which are processing the personal data of the data subject's request.
(66) オンライン環境における忘れられる権利を強化するため、削除の権利は、当該個人データを公開のものとした管理者が、当該個人データを取扱っている管理者に対して、当該個人データへのリンク、当該個人データのコピー又は複製物を消去するように通知することを義務付けられるというような方法によっても拡張されるべきである。そのようにする場合、当該管理者は、技術的な措置を含め、利用可能な技術及びその管理者にとって利用可能な方法を考慮に入れた上で、そのデータ主体の要求の対象である個人データを取扱っている管理者に対して通知をするための合理的な手立てを講じなければならない。

(67) Methods by which to restrict the processing of personal data could include, inter alia, temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website. In automated filing systems, the restriction of processing should in principle be ensured by technical means in such a manner that the personal data are not subject to further processing operations and cannot be changed. The fact that the processing of personal data is restricted should be clearly indicated in the system.
(67) 個人データの取扱いを制限するための方法は、特に、選別されたデータを一時的に他の取扱いシステムに移動すること、選別された個人データを利用者が利用できないようにすること、又は、公開されたデータを一時的に Web サイト上から削除することを含みうる。自動的なファイリングシステムにおいては、取扱いの制限は、原則として、その個人データが追加的取扱業務の対象とされないようにし、かつ、修正されないようにする態様で、技術的な手段によって確保されなければならない。個人データの取扱いが制限されているという事実は、そのシステムの中で明確に示されなければならない。

(68) To further strengthen the control over his or her own data, where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller. Data controllers should be encouraged to develop interoperable formats that enable data portability. That right should apply where the data subject provided the personal data on the basis of his or her consent or the processing is necessary for the performance of a contract. It should not apply where processing is based on a legal ground other than consent or contract. By its very nature, that right should not be exercised against controllers processing personal data in the exercise of their public duties. It should therefore not apply where the processing of the personal data is necessary for compliance with a

legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller. The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible. Where, in a certain set of personal data, more than one data subject is concerned, the right to receive the personal data should be without prejudice to the rights and freedoms of other data subjects in accordance with this Regulation. Furthermore, that right should not prejudice the right of the data subject to obtain the erasure of personal data and the limitations of that right as set out in this Regulation and should, in particular, not imply the erasure of personal data concerning the data subject which have been provided by him or her for the performance of a contract to the extent that and for as long as the personal data are necessary for the performance of that contract. Where technically feasible, the data subject should have the right to have the personal data transmitted directly from one controller to another.
(68) データ主体自身のデータに対するコントロールをより強化するため、個人データの取扱いが自動的な手段によって行われる場合、データ主体は、管理者に対して提供した当該データ主体と関係する個人データを、構造化され、一般的に利用され、機械可読性がありかつ相互運用可能なフォーマットで取得し、そして、これを別の管理者に対して移行できるようにもされなければならない。データ管理者は、データポータビリティを可能とする相互運用可能なフォーマットの開発を奨励されなければならない。この権利は、データ主体の同意に基づいて当該データ主体がその個人データを提供した場合、又は、契約の履行のためにその取扱いが必要となる場合に適用されなければならない。この権利は、その取扱いが同意又は契約以外の法的根拠に基づく場合には、適用されない。その性質上、この権利は、管理者の公的な義務の履行において個人データを取扱う管理者に対して、行使してはならない。それゆえ、この権利は、管理者が服すべき法的義務を遵守するために個人データの取扱いが必要となる場合、又は、公共の利益において、若しくは、管理者に与えられた公的な権限の行使において行われる職務の遂行のために個人データの取扱いが必要となる場合には、適用されない。自己と関係する個人データの移行又は受領というデータ主体の権利は、管理者に対して、技術的に互換性のある取扱いシステムの導入又は維持をすべき義務をつくり出すものではない。ある一群の個人データについて複数のデータ主体が関係している場合、個人データを受領する権利は、本規則に従い、他のデータ主体の権利及び自由を妨げてはならない。さらに、この権利は、個人データの削除を得るデータ主体の権利及び本規則に定める制限を妨げてはならず、また、特に、当該契約の履行のために必要となる範囲内で、かつ、その限りで、契約の履行のためにデータ主体から提供された、当該データ主体と関係する個人データの削除を意味するものではない。技術的に実現可能な場合において、データ主体は、ある管理者から別の管理者へと直接に個人データを移転させる権利を有するものとしなければならない。

(69) Where personal data might lawfully be processed because processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, or on grounds of the legitimate interests of a controller or a third party, a data subject should, nevertheless, be entitled to object to the processing of any personal data relating to his or her particular situation. It should be for the controller to demonstrate that its compelling legitimate interest overrides the interests or the fundamental rights and freedoms of the data subject.
(69) 公共の利益において、又は、管理者に与えられた公的な権限の行使において行われる職務の遂行のために取扱いが必要であるという理由で、又は、管理者若しくは第三者の正当な利益を根拠として、個人データが適法に取扱われうる場合、データ主体は、それにもかかわらず、自己の特別の状況に関する個人データの取扱いについて、異議を述べる資格が与えられなければならない。管理者は、管理者の必要不可欠の正当な利益がデータ主体の基本的な権利及び自由よりも優先することを証明しなければならない。

(70) Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing, including profiling to the extent that it is related to such direct marketing, whether with regard to initial or further processing, at any time and free of charge. That right should be explicitly brought to the attention of the data subject and presented clearly and separately from any other information.
(70) ダイレクトマーケティングの目的で個人データが取扱われる場合、そのダイレクトマーケティングと関連する範囲内にあるプロファイリングを含め、データ主体は、当初の取扱いと追加的取扱いのいずれに関しても、

いつでも、無償で、そのような取扱いを拒否する権利を有するものとしなければならない。この権利は、データ主体の目にとまるように明示されなければならず、また、明確に他の情報とは別に表示されなければならない。

(71) The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention. Such processing includes 'profiling' that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her. However, decision-making based on such processing, including profiling, should be allowed where expressly authorised by Union or Member State law to which the controller is subject, including for fraud and tax-evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller, or necessary for the entering or performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit consent. In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. Such measure should not concern a child.
In order to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal data are processed, the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect. Automated decision-making and profiling based on special categories of personal data should be allowed only under specific conditions.
(71) データ主体は、人間が介在しない与信申込みの自動的な拒否又は電子リクルート活動のような、自動的な取扱いのみに基づき、かつ、当該データ主体に関する法的効果を発生させ、又はデータ主体に対して同様の重大な影響を及ぼす、データ主体に関する個人的側面を評価する決定の対象とされない権利を有する。その決定は、措置を含みうる。そのような取扱いは、それが、データ主体に関して法的効果を発生させ、又は、データ主体に対して同様の重大な影響を及ぼす場合、特に、データ主体の業務遂行能力、経済状態、健康、個人的な嗜好又は興味、信頼性又は行動、位置又は移動に関する側面を分析又は予測するために、自然人に関する個人的側面を評価する個人データの何らかの形式の自動的な取扱いで構成される「プロファイリング」を含める。ただし、プロファイリングを含め、そのような取扱いに基づく決定は、EU の機関又は国内監視機関の規則、基準及び勧告に従って行われる不正行為及び脱税の監視及び防止のため、並びに、管理者によって提供されるサービスの安全性及び信頼性を確保するため、管理者が服する EU 法又は加盟国の国内法によって明確に承認される場合、又は、データ主体と管理者との間で契約を締結し、若しくは、それを履行するために必要な場合、又は、データ主体が明示の同意を与えた場合において認められるものとしなければならない。いずれの場合においても、そのような取扱いは、適切な保護措置に服するものとしなければならず、その保護措置は、データ主体に対する特別の情報提供、人間の介在を得る権利、当該データ主体の見解を表明する権利、そのような評価の後に到達した決定について説明を受ける権利、そして、その決定に対して異議を述べる権利を含むものでなければならない。そのような措置は、子どもと関係するものであってはならない。
　データ主体に関する公正かつ透明性のある取扱いを確保するために、その個人データが取扱われる具体的な状況及び過程を考慮に入れた上で、管理者は、プロファイリングのための適切な数学的又は統計的な手順を使用し、かつ、特に、個人データに不正確さをもたらす要素が補正され、エラーのリスクをミニマム化されるこ

とを確保し、データ主体の利益及び権利に含まれる潜在的なリスクを考慮に入れる態様で、そして、特に、自然人に対して、人種的若しくは民族的な出自、政治的な意見、信教若しくは信条、労働組合への加入、遺伝子の状態若しくは健康状態又は性的指向に基づく差別的効果が生ずることを避ける態様で、又は、措置がそのような効果を帰結することを避ける態様で、個人データを保護するための適切な技術上及び組織上の手段を実装しなければならない。特別な種類の個人データに基づく自動的な意思決定及びプロファイリングは、特定の条件に基づく場合においてのみ認められる。

(72) Profiling is subject to the rules of this Regulation governing the processing of personal data, such as the legal grounds for processing or data protection principles. The European Data Protection Board established by this Regulation (the 'Board') should be able to issue guidance in that context.
(72) プロファイリングは、取扱いの法的根拠又はデータ保護の基本原則のような、個人データの取扱いを規律する本規則の規定に服する。本規則によって設置される欧州データ保護会議（以下「欧州データ保護会議」という。）は、この文脈においてガイダンスを発行できるものとしなければならない。

(73) Restrictions concerning specific principles and the rights of information, access to and rectification or erasure of personal data, the right to data portability, the right to object, decisions based on profiling, as well as the communication of a personal data breach to a data subject and certain related obligations of the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of human life especially in response to natural or manmade disasters, the prevention, investigation and prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, or of breaches of ethics for regulated professions, other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, the keeping of public registers kept for reasons of general public interest, further processing of archived personal data to provide specific information related to the political behaviour under former totalitarian state regimes or the protection of the data subject or the rights and freedoms of others, including social protection, public health and humanitarian purposes. Those restrictions should be in accordance with the requirements set out in the Charter and in the European Convention for the Protection of Human Rights and Fundamental Freedoms.
(73) 特に自然災害又は人為的な災害への対応の際の人の生命の保護を含め、公共の安全への脅威、規制のある職業の倫理違反、又は、EU 若しくは加盟国の一般的な公共の利益の重要な対象、特に、EU 又は加盟国の重要な経済上若しくは財政上の利益に対する保護及びその防止を含め、犯罪行為の防止、捜査及び訴追又は刑罰の執行を保護するため、一般的な公共の利益を理由として保存される公的記録の維持管理、かつての全体主義国家体制の下での政治的活動に関する特別な情報を提供するための保管された個人データの追加的取扱い、又は、社会保障、公衆衛生及び人道上の目的を含め、データ主体の保護、又は、他者の権利及び自由を保護するために、民主主義社会において必要であり、かつ、比例的なものである限り、特定の基本原則、及び、情報提供の権利、個人データへのアクセス及びその訂正若しくは削除の権利、データポータビリティの権利、異議を述べる権利、プロファイリングに基づく決定、並びに、データ主体に対する個人データ侵害の連絡及び管理者の一定の関連義務に関し、EU 法若しくは加盟国の国内法により、制限を加えることができる。これらの制限は、憲章及び人権及び基本的な自由の保護のための欧州条約に定める要件に従わなければならない。

(74) The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.
(74) 管理者又は管理者の代わりの者によって行われる個人情報の取扱いに関し、管理者の職責及び法的責任が定められなければならない。特に、管理者は、適切かつ実効的な措置を実装すること、そして、その措置の実効性を含め、取扱活動が本規則を遵守していることを証明できるようにすることを義務付けられなければなら

ない。それらの措置は、取扱いの性質、範囲、過程及び目的、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なければならない。

(75) The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.
(75) 自然人の権利及び自由に対するリスクは、様々な蓋然性と深刻度で、個人データの取扱いから生じうる。それは、物的な損失、財産的な損失若しくは非財産的な損失を発生させうるものであり、特に：その取扱いが、差別、ID 盗取又は ID 詐欺、金銭上の損失、信用の毀損、職務上の守秘義務によって保護されている個人データの機密性の喪失、無権限による仮名化の復元、又は、それら以外の重大な経済的又は社会的な不利益を生じさせうる場合；データ主体がその権利及び自由を奪われ、又は、その個人データに対するコントロールの実行を妨げられる場合；人種的若しくは民族的な出自、政治的な意見、信教又は思想上の信条、労働組合の加入を明らかにする個人データの取扱い、並びに、遺伝子データ、健康と関係するデータ若しくは性生活と関係するデータ、又は、有罪判決及び犯罪行為若しくは関連する保護措置と関係するデータの取扱いの場合；個人的側面が評価される場合、特に、個人プロファイルの作成若しくはその使用のために、職務遂行能力、経済状態、健康、個人的な嗜好若しくは興味、信頼性若しくは行動、位置若しくは移動に関する側面が分析又は予測される場合；脆弱性のある自然人の個人データ、特に、子どもの個人データが取扱われる場合；又は、取扱いが莫大な量の個人データを含んでおり、多数のデータ主体に対して影響を及ぼす場合がそうである。

(76) The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk.
(76) データ主体の権利及び自由に対するリスクの蓋然性及びその深刻度は、その取扱いの性質、範囲、過程及び目的に照らして判断されなければならない。リスクは、データ取扱業務がリスク又は高度なリスクを含むものか否かを決めることのできる客観的な評価に基づいて決定されなければならない。

(77) Guidance on the implementation of appropriate measures and on the demonstration of compliance by the controller or the processor, especially as regards the identification of the risk related to the processing, their assessment in terms of origin, nature, likelihood and severity, and the identification of best practices to mitigate the risk, could be provided in particular by means of approved codes of conduct, approved certifications, guidelines provided by the Board or indications provided by a data protection officer. The Board may also issue guidelines on processing operations that are considered to be unlikely to result in a high risk to the rights and freedoms of natural persons and indicate what measures may be sufficient in such cases to address such risk.
(77) 特に、取扱いと関連するリスクの特定、その発生源、性質、蓋然性及び深刻度に関するリスク評価と関連して、適切な措置の実装及び管理者又は処理者による遵守の証明に関するガイド、並びに、リスクを削減するためのベストプラクティスの特定は、特に、承認された行動指針、承認された認証、データ保護機関から提供される運用指針又はデータ保護責任者から提供される指示によって、提供されうる。データ保護機関は、自然人の権利及び自由に対する高度なリスクを生じさせるおそれがないと判断される取扱業務に関する運用指針

を発行し、また、そのような場合において、そのようなリスクに対応するためにはどのような措置が十分なものとなりうるかを示すことができる。

(78) The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders.
(78) 個人データの取扱いと関連する自然人の権利及び自由の保護は、本規則の義務に適合することを確保するための適切な技術上及び組織上の措置が講じられることを要求する。本規則の遵守を証明できるようにするため、管理者は、内部的な基本原則を採択しなければならず、かつ、特に、データ保護バイデザインの原則及びデータ保護バイデフォルトの原則に適合する措置を実装しなければならない。そのような措置は、特に、個人データの取扱いの最小化、可能な限り速やかな個人データの仮名化、個人データの機能及び取扱いに関する透明性、データ主体がデータ取扱いを監視可能とすること、管理者が安全機能を開発し、向上させることを可能とすること、によって構成されうる。個人データの取扱いを基盤とし、又は、その職務を遂行するために個人データを取扱うアプリケーション、サービス及び製品を開発、設計、選択及び利用する場合、そのような製品、サービス及びアプリケーションの開発者は、そのような製品、サービス及びアプリケーションを開発及び設計する際、データ保護の権利を考慮に入れることが奨励され、また、最新技術を適正に考慮に入れた上で、管理者及び処理者がそのデータ保護義務を履行できるようにすることが奨励されなければならない。データ保護バイデザイン及びデータ保護バイデフォルトの原則は、公共入札の際においても考慮に入れられなければならない。

(79) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors, also in relation to the monitoring by and measures of supervisory authorities, requires a clear allocation of the responsibilities under this Regulation, including where a controller determines the purposes and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.
(79) データ主体の権利及び自由の保護並びに管理者及び処理者の義務及び法的責任は、管理者が他の管理者と共同して取扱いの目的及び方法を決定する場合、並びに、取扱業務が管理者の代わりに行われる場合を含め、監督機関による監視及び監督機関の措置との関係においても、本規則に基づく責任の明確な割り当てを必要とする。

(80) Where a controller or a processor not established in the Union is processing personal data of data subjects who are in the Union whose processing activities are related to the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union, or to the monitoring of their behaviour as far as their behaviour takes place within the Union, the controller or the processor should designate a representative, unless the processing is occasional, does not include processing, on a large scale, of special categories of personal data or the processing of personal data relating to criminal convictions and offences, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing or if the controller is a public authority or body. The representative should act on behalf of the controller or the processor and may be addressed by any supervisory authority. The representative should be explicitly designated by a written mandate of the controller or of the processor to act on its behalf

with regard to its obligations under this Regulation. The designation of such a representative does not affect the responsibility or liability of the controller or of the processor under this Regulation. Such a representative should perform its tasks according to the mandate received from the controller or processor, including cooperating with the competent supervisory authorities with regard to any action taken to ensure compliance with this Regulation. The designated representative should be subject to enforcement proceedings in the event of non-compliance by the controller or processor.
(80) EU 域内に拠点のない管理者又は処理者が、EU 域内のデータ主体の個人データを取扱っており、その取扱活動が、データ主体による支払いが必要とされると否とにかかわらず、そのような EU 域内のデータ主体に対する物品又はサービスの提供と関連するものである場合、又は、EU 域内で起きる行動である限りにおいてデータ主体の行動の監視と関連するものである場合、その取扱いが、偶発的なものであり、特別な種類のデータの取扱いを大規模に含んでいないか、又は有罪判決及び犯罪行為と関連する個人データの取扱いを含んでいない場合であって、取扱いの性質、過程、範囲及び目的を考慮に入れた上で、自然人の権利及び自由に対するリスクを発生させるおそれがない場合、又は、その管理者が公的機関若しくは公的組織である場合を除き、その管理者又は処理者は、代理人を指定しなければならない。代理人は、管理者又は処理者の代わりに行動しなければならず、かつ、監督機関からの名宛人となることができる。代理人は、本規則に基づく管理者又は処理者の義務に関し、それらの者の代わりに行動することの管理者又は処理者の書面による委任によって、明示的に指定されなければならない。そのような代理人の指定は、本規則に基づく管理者及び処理者の義務又は法的責任に影響を与えることはない。そのような代理人は、本規則の遵守を確保するために行われる全ての行為に関する職務権限をもつ監督機関との協力を含め、管理者又は処理者から受けた委任に従って、その職務を遂行しなければならない。指定された代理人は、管理者又は処理者による違背行為が発生した場合には、法執行の手続に服さなければならない。

(81) To ensure compliance with the requirements of this Regulation in respect of the processing to be carried out by the processor on behalf of the controller, when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of this Regulation, including for the security of processing. The adherence of the processor to an approved code of conduct or an approved certification mechanism may be used as an element to demonstrate compliance with the obligations of the controller. The carrying-out of processing by a processor should be governed by a contract or other legal act under Union or Member State law, binding the processor to the controller, setting out the subject-matter and duration of the processing, the nature and purposes of the processing, the type of personal data and categories of data subjects, taking into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk to the rights and freedoms of the data subject. The controller and processor may choose to use an individual contract or standard contractual clauses which are adopted either directly by the Commission or by a supervisory authority in accordance with the consistency mechanism and then adopted by the Commission. After the completion of the processing on behalf of the controller, the processor should, at the choice of the controller, return or delete the personal data, unless there is a requirement to store the personal data under Union or Member State law to which the processor is subject.
(81) 管理者の代わりに処理者によって行われる取扱いに関する本規則の義務の遵守を確保するため、管理者は、処理者に対して取扱活動を委託する場合、取扱いの安全性に関するものを含め、本規則の義務に適合する技術上及び組織上の措置の実装を、特に専門知識、信頼性及び資源の面において十分に保証する処理者のみを使用しなければならない。承認された行動準則又は承認された認証方法を処理者が遵守していることは、管理者の義務の遵守を示すための要素として用いられうる。処理者による取扱いの実施は、処理者と管理者とを拘束し、行われる取扱いの過程における処理者の特定された職務及び職責並びにデータ主体の権利及び自由に対するリスクを考慮に入れた上で、取扱いの対象及び期間、取扱いの性質及び目的、個人データの種類及びデータ主体の類型を定める契約又は EU 法若しくは加盟国の国内法に基づくその他の法律行為によって規律されなければならない。管理者及び処理者は、個別の契約、又は、欧州委員会によって直接に採択された標準約款、若しくは、一貫性メカニズムに従って監督機関により採択され、欧州委員会によって承認された標準約款の利用を選択しうる。管理者の代わりの取扱いを完了した後、その処理者が服する EU 法又は加盟国の国内法に基

づいて当該個人データを記録保存すべき義務が存在しない限り、処理者は、管理者の選択により、その個人データを返却し、又は、これを削除しなければならない。

(82) In order to demonstrate compliance with this Regulation, the controller or processor should maintain records of processing activities under its responsibility. Each controller and processor should be obliged to cooperate with the supervisory authority and make those records, on request, available to it, so that it might serve for monitoring those processing operations.
(82) 本規則の遵守を証明するために、管理者又は処理者は、その責任において、取扱活動の記録を保管しなければならない。個々の管理者及び処理者は、監督機関と協力し、かつ、その要求に基づき、監督機関がその取扱業務の監視の任を果たしうるようにするため、それらの記録を監督機関が利用できるようにすることを義務付けられる。

(83) In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.
(83) 安全性を維持管理するため、そして、本規則の違反となる取扱いを防止するため、管理者又は処理者は、その取扱いに内在するリスクを評定しなければならず、また、暗号化のような、それらのリスクを削減するための手段を実装しなければならない。その手段は、最新技術及びそのリスクと保護されるべき個人データの性質との関連における実装費用を考慮に入れた上で、機密性を含め、適切なレベルの安全性を確保するものでなければならない。データのセキュリティ上のリスクの評価に際しては、送信され、記録保存され、又は、それ以外の取扱いをされる個人データの偶発的又は違法な破壊、喪失、改変、無権限の開示又は無権限のアクセスのような、個人データの取扱いによってもたらされ、特に物的な損失、財産的若しくは非財産的な損失を発生させるかもしれないリスクについて、検討が加えられなければならない。

(84) In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk. The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation. Where a data-protection impact assessment indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing.
(84) 取扱業務によって自然人の権利及び自由に対する高度なリスクが生ずるおそれのある場合に対して本規則の遵守を強化するために、管理者は、特に、そのリスクの発生源、性質、特性及び深刻度を評価するためのデータ保護影響評価を行うべき責任を負う。その評価結果は、その個人データの取扱いが本規則を遵守するものであることを証明するための適切な措置がどの時点で定められたのかを考慮に入れなければならない。利用可能な技術及び実施費用の観点から管理者が適切な措置によって低減させることのできない高いリスクがその取扱業務に含まれているということをそのデータ保護影響評価が示す場合、その取扱いを開始する前に、監督機関との協議を行わなければならない。

(85) A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned. Therefore, as soon as the controller becomes 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.
(85) 個人データ侵害は、適切かつ適時の態様で対応が行われないと、自然人の個人データに対する管理の欠落又は自然人の権利制限の喪失、差別、ID 盗取又は ID 詐欺、金銭上の損失、無権限による仮名の復元、信用の毀損、職務上の守秘義務によって保護された個人データの機密性の喪失、又は、関係する自然人に対するその他の重要な経済的若しくは社会的不利益といったような、自然人に対する物的な損失、財産的な損失若しくは非財産的な損失をもたらしうる。それゆえ、個人データ侵害が発生したことに管理者が気づいたならば可能な限り速やかに、説明責任の原則に従い、その個人データ侵害が自然人の権利及び自由に対するリスクを発生させるおそれがないということを管理者が証明できる場合を除き、その管理者は、監督機関に対し、不当な遅滞なく、かつ、それが可能であるときは、それに気づいた時から遅くとも 72 時間以内に、その個人データ侵害を通知しなければならない。72 時間以内にその通知を完了できない場合、その遅延の理由をその通知に付さなければならず、そして、更なる不当な遅延なく、同時に情報を提供しうる。

(86) The controller should communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person in order to allow him or her to take the necessary precautions. The communication should describe the nature of the personal data breach as well as recommendations for the natural person concerned to mitigate potential adverse effects. Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities. For example, the need to mitigate an immediate risk of damage would call for prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication.
(86) 管理者は、当該個人データ侵害が自然人の権利及び自由に対する高いリスクを発生させるおそれがあるときは、当該個人が予め必要な予防策を講じることができるように、データ主体に対し、不当な遅滞なく、個人データ侵害について連絡しなければならない。その連絡は、個人データ侵害の性質、並びに、関係する自然人に向けた潜在的な悪影響を低減するための勧告を記述しなければならない。そのようなデータ主体に対する連絡は、監督機関から提供されたガイダンス又は法執行機関のような監督機関以外の関連機関から提供されたガイダンスを尊重しつつ、可能な限り速やかに合理的に実現できるように、かつ、監督機関と密接に協力して、行われなければならない。例えば、損害発生の緊急のリスクを低減させる必要性があることは、データ主体への連絡を督促することになるが、他方、個人データ侵害の継続又は類似の侵害の発生に対抗するための適切な措置の実施の必要性があることは、さらに連絡する時間がかかることを正当化しうる。

(87) It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject. The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation.
(87) 個人データ侵害が発生したかどうかを迅速に確定するため、そして、監督機関及びデータ主体に対して速やかに連絡するための全ての適切な技術的な保護及び組織上の措置が実装されているか否かが確認されなければならない。特に、その個人データ侵害の性質及び重大性、その結果として生じる事態及びデータ主体に対する悪影響を考慮に入れた上で、不当な遅滞なく通知が行われたという事実が立証されなければならない。そのような通知は、本規則に定める監督機関の職務及び権限に従い、監督機関の介入を招くものとなりうる。

(88) In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches,

due consideration should be given to the circumstances of that breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse. Moreover, such rules and procedures should take into account the legitimate interests of law-enforcement authorities where early disclosure could unnecessarily hamper the investigation of the circumstances of a personal data breach.
(88) 個人データ侵害の通知に適用可能なフォーマット及び手続と関係する規定を設ける際、ID 詐欺又はそれ以外の形式による濫用行為が発生するおそれを実効的に抑制する適切な技術的保護措置によって個人データが保護されていたか否かを含め、個人データ侵害の状況について、十分な検討が加えられなければならない。さらに、そのような規定及び手続は、早い段階における開示が個人データ侵害の状況に関する捜査を不必要に妨げてしまう場合、法執行機関の正当な利益を考慮に入れなければならない。

(89) Directive 95/46/EC provided for a general obligation to notify the processing of personal data to the supervisory authorities. While that obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Such indiscriminate general notification obligations should therefore be abolished, and replaced by effective procedures and mechanisms which focus instead on those types of processing operations which are likely to result in a high risk to the rights and freedoms of natural persons by virtue of their nature, scope, context and purposes. Such types of processing operations may be those which in, particular, involve using new technologies, or are of a new kind and where no data protection impact assessment has been carried out before by the controller, or where they become necessary in the light of the time that has elapsed since the initial processing.
(89) 指令 95/46/EC は、監督機関に対して個人データの取扱いを通知すべき一般的な義務を定めた。その義務は、管理上及び資金上の問題を生じさせる一方で、全ての場合において、個人データ保護の向上に寄与しなかった。それゆえ、そのような無限定の一般的な通知義務は廃止されなければならず、そして、それに代えて、取扱業務の性質、範囲、過程及び目的のゆえに自然人の権利及び自由に対する高いリスクをもたらすことが予想される種類の取扱業務に焦点を絞った実効的な手続及び仕組みによって置き換えられるべきである。そのような種類の取扱業務は、特に、その中に新たな技術又は新たな種類の技術の利用を含む取扱業務であり、そして、管理者によるデータ保護影響評価がこれまで行われたことがなく、又は、最初の取扱いの時から経過した時日に照らし、データ保護影響評価が必要となった取扱業務でありうる。

(90) In such cases, a data protection impact assessment should be carried out by the controller prior to the processing in order to assess the particular likelihood and severity of the high risk, taking into account the nature, scope, context and purposes of the processing and the sources of the risk. That impact assessment should include, in particular, the measures, safeguards and mechanisms envisaged for mitigating that risk, ensuring the protection of personal data and demonstrating compliance with this Regulation.
(90) そのような場合において、取扱いが行われる前に、取扱いの性質、範囲、文脈及び目的並びにリスクの発生源を考慮に入れた上で、高いリスクの特定の蓋然性及び深刻度を評価するために、管理者によって、データ保護影響評価が行われなければならない。その影響評価は、特に、そのリスクを低減し、個人データの保護を確保し、そして、本規則の遵守を証明するために準備された措置、保護措置及び仕組みを含めなければならない。

(91) This should in particular apply to large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk, for example, on account of their sensitivity, where in accordance with the achieved state of technological knowledge a new technology is used on a large scale as well as to other processing operations which result in a high risk to the rights and freedoms of data subjects, in particular where those operations render it more difficult for data subjects to exercise their rights. A data protection impact assessment should also be made where personal data are processed for taking decisions regarding specific natural persons following any systematic and extensive evaluation of personal aspects relating to natural persons based on profiling those data or following the processing of special categories of personal data, biometric data, or data on criminal convictions and offences or related security measures. A data protection impact assessment

is equally required for monitoring publicly accessible areas on a large scale, especially when using optic-electronic devices or for any other operations where the competent supervisory authority considers that the processing is likely to result in a high risk to the rights and freedoms of data subjects, in particular because they prevent data subjects from exercising a right or using a service or a contract, or because they are carried out systematically on a large scale. The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer. In such cases, a data protection impact assessment should not be mandatory.
(91) このことは、特に、地域レベル、国家レベル及び多国間レベルの非常に大きな分量の個人データの取扱いを対象とし、大勢のデータ主体に対して悪影響を及ぼすおそれがあり、かつ、例えば、その機微性ゆえに高いリスクをもたらすことが予想され、かつ、達成された技術知識に従って新技術が大規模に利用される大規模な取扱業務に対して、並びに、それ以外の、データ主体の権利及び自由に対して高いリスクをもたらすことが予想される取扱業務、特に、それらの取扱業務がデータ主体による自らの権利の行使をより困難にしている取扱業務に対して適用されなければならない。それらのデータのプロファイリングに基づく自然人に関する個人的な側面が体系的に、広範囲に及ぶ評価を伴う、あるいは、特別な種類特別な種類の個人データ、生体データ、又は、有罪判決及び犯罪若しくは関連する安全管理措置に関するデータの取扱いを伴う特定の自然人に関する評価を行うために個人データが取扱われる場合においても、データ保護影響評価が実施されなければならない。公衆がアクセス可能な場所の大規模な監視、特に光学・電子機器を用いて行われる場合に関しても、又は、特に、データ主体が権利の行使やサービス若しくは契約の利用を妨げられているという理由により、あるいは、その取扱いが大規模に体系的に行われているという理由により、データ主体の権利及び自由に高いリスクをもたらす可能性があると所管監督機関が判断する場合、上記以外の全ての業務についても、同等に、データ保護影響評価が要求される。その取扱いが患者又は顧客からの個人データに関するものであり、個々の医師、その他の医療専門職又は法律家による場合、その個人データの取扱いは、大規模なものと判断されてはならない。そのような場合、データ保護影響評価は、義務ではない。

(92) There are circumstances under which it may be reasonable and economical for the subject of a data protection impact assessment to be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity.
(92) データ保護影響評価の対象を単独の評価計画による場合よりも拡張したほうが合理的で経済的なものとなりうるような場合がある。例えば、公的機関又は団体が共通のアプリケーション又は取扱プラットフォームの構築を予定する場合、又は、複数の管理者が、産業部門若しくは業界を横断して、あるいは、広範に利用されている横断的な活動のために、共通のアプリケーション又は取扱環境の導入を計画する場合がそうである。

(93) In the context of the adoption of the Member State law on which the performance of the tasks of the public authority or public body is based and which regulates the specific processing operation or set of operations in question, Member States may deem it necessary to carry out such assessment prior to the processing activities.
(93) 公的機関及び団体の職務遂行の根拠となり、かつ、当の特定の取扱業務又は一群の取扱業務を規制する加盟国法の採択の過程において、加盟国は、取扱活動を行う前にそのような評価を行う必要性があると判断できる。

(94) Where a data protection impact assessment indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation, the supervisory authority should be consulted prior to the start of processing activities. Such high risk is likely to result from certain types of processing and the extent and frequency of processing, which may result also in a realisation of damage or interference with the rights and freedoms of the natural person. The supervisory authority should respond to the request for consultation within a specified period. However, the absence of a reaction of the supervisory authority within that period should be without prejudice to any intervention of the supervisory authority in accordance with its

tasks and powers laid down in this Regulation, including the power to prohibit processing operations. As part of that consultation process, the outcome of a data protection impact assessment carried out with regard to the processing at issue may be submitted to the supervisory authority, in particular the measures envisaged to mitigate the risk to the rights and freedoms of natural persons.
(94) リスクを低減するための保護措置、安全管理措置及び仕組みを欠くときは、その取扱いが自然人の権利及び自由に対する高いリスクをもたらしうるということをデータ保護影響評価が示しており、かつ、利用可能な技術及びその実施費用の観点から合理的な手段によってはそのリスクを低減できないという意見をその管理者がもつ場合、監督機関は、取扱活動を開始する前に協議を受けるものとしなければならない。自然人の権利及び自由に対する被害又は妨害を現実に発生させうるような高度のリスクは、一定の種類の取扱い、取扱いの範囲及び頻度から生ずる可能性がある。監督機関は、所定の期間内に、協議の要求に対応しなければならない。ただし、当該期間内に監督機関から何らの応答もないことは、取扱業務を禁止する権限を含め、本規則に定める監督機関の職務及び権限に従った監督機関の介入を妨げない。その協議過程の一部として、監督機関に対し、問題となる取扱いに関して行われたデータ保護影響評価の結果、特に、自然人の権利及び自由に対するリスクを低減するために想定された措置に関する評価結果を提出しうる。

(95)The processor should assist the controller, where necessary and upon request, in ensuring compliance with the obligations deriving from the carrying out of data protection impact assessments and from prior consultation of the supervisory authority.
(95) 処理者は、必要なときは、かつ、要求に応じて、データ保護影響評価を行うことから派生する義務及び監督機関の事前協議から派生する義務の遵守を確保する際、管理者を支援しなければならない。

(96) A consultation of the supervisory authority should also take place in the course of the preparation of a legislative or regulatory measure which provides for the processing of personal data, in order to ensure compliance of the intended processing with this Regulation and in particular to mitigate the risk involved for the data subject.
(96) 監督機関との協議は、予定されている取扱いの本規則への遵守を確保するため、及び、特に、データ主体のために内在するリスクを低減するため、個人データの取扱いを定める立法又は規制上の措置を準備する過程においても行われなければならない。

(97) Where the processing is carried out by a public authority, except for courts or independent judicial authorities when acting in their judicial capacity, where, in the private sector, processing is carried out by a controller whose core activities consist of processing operations that require regular and systematic monitoring of the data subjects on a large scale, or where the core activities of the controller or the processor consist of processing on a large scale of special categories of personal data and data relating to criminal convictions and offences, a person with expert knowledge of data protection law and practices should assist the controller or processor to monitor internal compliance with this Regulation. In the private sector, the core activities of a controller relate to its primary activities and do not relate to the processing of personal data as ancillary activities. The necessary level of expert knowledge should be determined in particular according to the data processing operations carried out and the protection required for the personal data processed by the controller or the processor. Such data protection officers, whether or not they are an employee of the controller, should be in a position to perform their duties and tasks in an independent manner.
(97) 裁判所又は独立司法機関がその司法上の権能において行動する場合を除き、取扱いが公的機関によって行われる場合、民間部門において、定期的に体系的にデータ主体を大規模に監視することを要する取扱業務を中心的な業務とする管理者によって取扱いが行われる場合、又は、管理者及び処理者の中心的な業務が、特別な種類の個人データ並びに有罪判決及び犯罪と関連するデータの大規模な取扱いによって構成されている場合、本規則の内部的な遵守を監視するために、データ保護法令及びその実務に関する専門知識をもつ者が管理者又は処理者を支援しなければならない。民間部門においては、管理者の中心的業務は、その基本的な活動と関連するものであり、付随的な業務としての個人データの取扱いと関連するものではない。必要とされる専門知識のレベルは、特に、行われるデータ取扱業務に従って、そして、管理者又は処理者によって取扱われる個人データにとって必要な保護に従って、決定されなければならない。そのようなデータ保護オフィサーは、管理者

の従業者であるか否かを問わず、独立の態様でその義務及び職務を遂行するための地位を有するものとしなければならない。

(98) Associations or other bodies representing categories of controllers or processors should be encouraged to draw up codes of conduct, within the limits of this Regulation, so as to facilitate the effective application of this Regulation, taking account of the specific characteristics of the processing carried out in certain sectors and the specific needs of micro, small and medium enterprises. In particular, such codes of conduct could calibrate the obligations of controllers and processors, taking into account the risk likely to result from the processing for the rights and freedoms of natural persons.
(98) 一定の部門において行われる取扱いの特殊性並びに中小零細企業の特殊事情を考慮に入れた上で、本規則の効果的な適用を促進するために、様々な種類の管理者又は処理者を代表する団体その他の組織は、本規則の制限内で、行動準則を作成することが奨励されなければならない。特に、そのような行動準則は、取扱いの結果として発生するおそれのある自然人の権利及び自由に対するリスクを考慮に入れた上で、管理者及び処理者の義務を調整しうる。

(99) When drawing up a code of conduct, or when amending or extending such a code, associations and other bodies representing categories of controllers or processors should consult relevant stakeholders, including data subjects where feasible, and have regard to submissions received and views expressed in response to such consultations.
(99) 行動準則を作成する際、又は、その準則を改正又は追補する際、様々な種類の管理者又は処理者を代表する団体その他の組織は、それが有用であるときはデータ主体を含め、関係する利害関係者と協議し、そして、そのような協議に応じて申し出や表明された意見を考慮しなければならない。

(100) In order to enhance transparency and compliance with this Regulation, the establishment of certification mechanisms and data protection seals and marks should be encouraged, allowing data subjects to quickly assess the level of data protection of relevant products and services.
(100) 透明性及び本規則の遵守を拡大するために、関連する製品及びサービスのデータ保護水準をデータ主体が即座に評価できるようにする認証方法、データ保護シール及びデータ保護マークを設けることが促進されなければならない。

(101) Flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation. The increase in such flows has raised new challenges and concerns with regard to the protection of personal data. However, when personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation. In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation. A transfer could take place only if, subject to the other provisions of this Regulation, the conditions laid down in the provisions of this Regulation relating to the transfer of personal data to third countries or international organisations are complied with by the controller or processor.
(101) EU 域外の国々及び国際機関への個人データの流通並びにこれらのところからの個人データの流通は、国際取引及び国際協力を拡大するために必要なものである。そのような流通の増加は、個人データの保護に関する新たな検討課題と懸念を発生させてきた。ただし、EU から第三国又は国際機関の中に所在する管理者、処理者若しくはそれ以外の取得者に対して個人データが移転される場合、その第三国又は国際機関から同じ第三国若しくは国際機関内の管理者や処理者又は別の第三国若しくは国際機関の管理者や処理者に対して個人データが転送される場合を含め、本規則によって EU 域内で確保される自然人の保護の水準を低下させるべきではない。いずれの場合においても、第三国及び国際機関への移転は、本規則を完全に遵守する場合においてのみ、これを行うことができる。本規則の別の条項に従い、第三国又は国際機関へ個人データを移転するための本規則の条項中に定める要件が管理者又は処理者によって遵守される場合においてのみ、その移転をすること

ができる。

(102) This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subjects. Member States may conclude international agreements which involve the transfer of personal data to third countries or international organisations, as far as such agreements do not affect this Regulation or any other provisions of Union law and include an appropriate level of protection for the fundamental rights of the data subjects.
(102) 本規則は、データ主体のための適切な保護措置を含め、個人データの移転を規制する EU と第三国との間で締結される国際協定を妨げない。加盟国は、そのような協定が本規則又はそれ以外の EU 法の条項に影響を与えることがなく、かつ、データ主体の基本的な権利のための適切な水準の保護を含めている場合に限り、第三国又は国際機関への個人データの移転を含む国際協定を締結できる。

(103) The Commission may decide with effect for the entire Union that a third country, a territory or specified sector within a third country, or an international organisation, offers an adequate level of data protection, thus providing legal certainty and uniformity throughout the Union as regards the third country or international organisation which is considered to provide such level of protection. In such cases, transfers of personal data to that third country or international organisation may take place without the need to obtain any further authorisation. The Commission may also decide, having given notice and a full statement setting out the reasons to the third country or international organisation, to revoke such a decision.
(103) 欧州委員会は、十分なレベルの保護を提供するものと判断される第三国又は国際機関に関しては、第三国、第三国内の地域若しくは特定の部門又は国際機関が十分なレベルのデータ保護を提供しており、そして、EU 全域における法的安定性及び統一性を提供している旨の決定を EU 全域において有効なものとして、行うことができる。その場合、当該第三国又は国際機関への個人データの移転は、別の承認を得る必要なく、これを行うことができる。欧州委員会は、その第三国又は国際機関に対し、その通知及びその理由の全文を示す声明文を発して、その決定を無効にする決定を行うこともできる。

(104) In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of the third country, or of a territory or specified sector within a third country, take into account how a particular third country respects the rule of law, access to justice as well as international human rights norms and standards and its general and sectoral law, including legislation concerning public security, defence and national security as well as public order and criminal law. The adoption of an adequacy decision with regard to a territory or a specified sector in a third country should take into account clear and objective criteria, such as specific processing activities and the scope of applicable legal standards and legislation in force in the third country. The third country should offer guarantees ensuring an adequate level of protection essentially equivalent to that ensured within the Union, in particular where personal data are processed in one or several specific sectors. In particular, the third country should ensure effective independent data protection supervision and should provide for cooperation mechanisms with the Member States' data protection authorities, and the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress.
(104) EU が立脚する基本的な価値観、特に、人権の保護に沿って、欧州委員会は、その第三国又はその第三国内の地域若しくは特定の部門の評価に際し、特定の第三国が、法の支配、司法へのアクセス、並びに、国際人権の規範と基準、及び、公共の安全、国防及び国家安全保障並びに公共の秩序及び刑事法に関する立法を含め、その第三国の一般法及び特別法をいかに尊重しているかを考慮に入れなければならない。第三国内の地域又は特定の部門と関連する十分性決定の採択は、特定の取扱活動及びその第三国において施行されている適用可能な法的基準及び立法の適用範囲のような、明確で客観的な基準を考慮に入れなければならない。特に、個人データが一又は複数の特定の部門において取扱われる場合において、その第三国は、EU 域内で確保されている保護と基本的に等しく十分なレベルの保護を確保していることの保証を提供しなければならない。特に、その第三国は、実効的かつ独立のデータ保護監督を確保しなければならず、かつ、加盟国のデータ保護機関との協力の仕組みを定めなければならず、かつ、データ主体は、実効的で執行可能な権利並びに実効的な行政救済及び司法救済を与えられるものとしなければならない。

(105) Apart from the international commitments the third country or international organisation has entered into, the Commission should take account of obligations arising from the third country's or international organisation's participation in multilateral or regional systems in particular in relation to the protection of personal data, as well as the implementation of such obligations. In particular, the third country's accession to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data and its Additional Protocol should be taken into account. The Commission should consult the Board when assessing the level of protection in third countries or international organisations.
(105) 第三国又は国際機関が加入している国際関係とは別に、欧州委員会は、特に、個人データの保護並びにその義務の履行と関連して、第三国又は国際機関が多国間のシステム又は地域的なシステムに参加することから生ずる義務を考慮しなければならない。特に、個人データの自動的な取扱いに関連する個人の保護のための1981年1月28日の欧州評議会条約及びその追加議定書への第三国の加盟を考慮に入れなければならない。欧州委員会は、第三国及び国際機関における保護の水準を評価する際、委員会と協議しなければならない。

(106) The Commission should monitor the functioning of decisions on the level of protection in a third country, a territory or specified sector within a third country, or an international organisation, and monitor the functioning of decisions adopted on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC. In its adequacy decisions, the Commission should provide for a periodic review mechanism of their functioning. That periodic review should be conducted in consultation with the third country or international organisation in question and take into account all relevant developments in the third country or international organisation. For the purposes of monitoring and of carrying out the periodic reviews, the Commission should take into consideration the views and findings of the European Parliament and of the Council as well as of other relevant bodies and sources. The Commission should evaluate, within a reasonable time, the functioning of the latter decisions and report any relevant findings to the Committee within the meaning of Regulation (EU) No 182/2011 of the European Parliament and of the Council [12] as established under this Regulation, to the European Parliament and to the Council.
(106) 欧州委員会は、第三国、第三国内の地域若しくは特定の部門又は国際機関における保護のレベルに関する決定が有効に機能していることを監視しなければならず、また、指令95/46/ECの第25条第6項又は第26条第4項に基づいて採択された決定が有効に機能していることを監視しなければならない。この十分性の決定において、欧州委員会は、それらが有効に機能していることを定期的に見直す仕組みを定めなければならない。この定期的な見直しは、当の第三国又は国際機関との協議を経た上で、その第三国又は国際機関内の関連する全ての動向を考慮に入れた上で、行われなければならない。この監視及び定期的な見直しを行う目的のために、欧州委員会は、欧州議会及び理事会並びにそれ以外の関連する組織や情報源からの意見及び判断を考慮に入れなければならない。欧州委員会は、合理的な期間内に、後者の決定が有効に機能していることを評価し、かつ、本規則に基づいて策定されたものとしての欧州議会及び理事会の規則(EU) No 182/2011[12]の意味における委員会、欧州議会及び理事会に対し、その調査結果を報告しなければならない。

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

[12] Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).
欧州委員会の実装権限の行使の加盟国による管理のための制度に関する規則及び一般原則を定める欧州議会及び理事会の2011年2月16日の規則(EU) No 182/2011（OJ L 55, 28.2.2011, p. 13）

(107) 欧州委員会は、第三国、第三国内の地域若しくは特定の部門又は国際機関が十分な水準のデータ保護をもはや確保していない旨を判断できる。その判断の結果、当該第三国又は国際機関に対する個人データの移転は、拘束的企業準則を含め、適切な保護措置による移転及び特別な状況における例外に関する本規則の要件が充足されない限り、禁止されなければならない。この場合、欧州委員会と当該第三国又は国際機関との間で、協議がもたれなければならない。欧州委員会は、その状況を救済するため、適時に、その第三国又は国際機関に対し、その理由を通知し、かつ、協議に入らなければならない。

(108) In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or contractual clauses authorised by a supervisory authority. Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union, including the availability of enforceable data subject rights and of effective legal remedies, including to obtain effective administrative or judicial redress and to claim compensation, in the Union or in a third country. They should relate in particular to compliance with the general principles relating to personal data processing, the principles of data protection by design and by default. Transfers may also be carried out by public authorities or bodies with public authorities or bodies in third countries or with international organisations with corresponding duties or functions, including on the basis of provisions to be inserted into administrative arrangements, such as a memorandum of understanding, providing for enforceable and effective rights for data subjects. Authorisation by the competent supervisory authority should be obtained when the safeguards are provided for in administrative arrangements that are not legally binding.
(108) 十分性認定がない場合、管理者又は処理者は、データ主体のための適切な保護措置という方法によって、第三国内におけるデータ保護の欠落を補う措置を講じなければならない。そのような適切な保護措置は、拘束的企業準則、欧州委員会によって採択された標準データ保護条項、監督機関によって採択された標準データ保護条項、又は、監督機関によって承認された契約条項によって構成されうる。それらの保護措置は、データ主体の執行可能な権利を利用できること、並びに、実効的な行政救済又は司法救済を得るためのもの及び損害賠償を請求するためのものを含む実効的な司法救済を利用できることを含め、EU 域内における取扱いにとって適切なデータ保護上の義務の遵守並びにデータ主体の権利及び自由を、EU 域内又は第三国内において確保するものでなければならない。それらは、特に、個人データの取扱いと関連する一般的な基本原則、データ保護バイデザインの原則及びデータ保護バイデフォルトの原則の遵守と関連するものでなければならない。公的機関又は公的組織は、確認覚書のような行政文書の中に挿入されたデータ主体のための執行可能で実効的な権利を定める条項に基づく場合を含め、第三国又は国際機関内において対応する職責及び権能をもつ公的機関又は公的組織との間で移転を行うこともできる。保護措置が法的拘束力のない行政文書によって定められている場合、所轄監督機関による承認を受けなければならない。

(109) The possibility for the controller or processor to use standard data-protection clauses adopted by the Commission or by a supervisory authority should prevent controllers or processors neither from including the standard data-protection clauses in a wider contract, such as a contract between the processor and another processor, nor from adding other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects. Controllers and processors should be encouraged to provide additional safeguards via contractual commitments that supplement standard protection clauses.
(109) 欧州委員会又は監督機関によって採択された標準データ保護約款を管理者又は処理者が利用することができるということは、欧州委員会又は監督機関によって採択された標準契約条項と直接又は間接に矛盾せず、かつ、データ主体の基本的な権利及び自由を妨げるものではない限り、管理者又は処理者が、処理者と別の処理者との間の契約のような、より広範囲の契約の中に標準データ保護条項を含めることを妨げるものではなく、また、その約款の中に別の条項や保護措置を追加することを妨げるものでもない。管理者及び処理者は、標準データ保護条項を補完する契約上の約定を介して、追加的な保護措置を提供することが奨励されなければなら

ない。

(110) A group of undertakings, or a group of enterprises engaged in a joint economic activity, should be able to make use of approved binding corporate rules for its international transfers from the Union to organisations within the same group of undertakings, or group of enterprises engaged in a joint economic activity, provided that such corporate rules include all essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data.
(110) 企業グループ又は共同で経済活動に従事する企業グループは、そのような拘束的企業準則が、個人データの移転又はその移転の種類のための適切な保護措置を確保するための全ての重要な基本原則及び執行可能な権利を含めるものである限り、EU から同じ企業グループ又は共同で経済活動に従事する企業グループ内にある組織に対する個人データの国際的な移転のために、承認された拘束的企業準則を利用できるようにしなければならない。

(111) Provisions should be made for the possibility for transfers in certain circumstances where the data subject has given his or her explicit consent, where the transfer is occasional and necessary in relation to a contract or a legal claim, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies. Provision should also be made for the possibility for transfers where important grounds of public interest laid down by Union or Member State law so require or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest. In the latter case, such a transfer should not involve the entirety of the personal data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or, if they are to be the recipients, taking into full account the interests and fundamental rights of the data subject.
(111) データ主体が自己の明示の同意を与えたという一定の状況下において、規制当局の手続を含め、それが司法手続内のものであるか行政手続若しくは訴訟外手続によるものであるかを問わず、契約又は訴訟との関係において、その移転が偶発的なものであり、かつ、必要なものである場合、移転を可能とするための条項が設けられなければならない。EU 法又は加盟国法によって定められる公共の利益上の重要な法的根拠がそのような移転を求める場合、又は、法律によって策定され、正当な利益を有する公的若しくは個人からの協議に応ずるための登録所から移転が行われる場合において、移転ができるようにするための条項も設けられなければならない。後者の場合、そのような移転は、その登録所の中に収められている個人データ全体又はデータの種類全体を含めることはできず、かつ、正当な利益をもつ個人からの協議に対して登録所が応じようとする場合には、そのような者の要求があった際においてのみ、又は、それが取得者のために行われる場合には、データ主体の利益及び基本的な権利を完全に考慮に入れた上で、移転が行われるものとしなければならない。

(112) Those derogations should in particular apply to data transfers required and necessary for important reasons of public interest, for example in cases of international data exchange between competition authorities, tax or customs administrations, between financial supervisory authorities, between services competent for social security matters, or for public health, for example in the case of contact tracing for contagious diseases or in order to reduce and/or eliminate doping in sport. A transfer of personal data should also be regarded as lawful where it is necessary to protect an interest which is essential for the data subject's or another person's vital interests, including physical integrity or life, if the data subject is incapable of giving consent. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of data to a third country or an international organisation. Member States should notify such provisions to the Commission. Any transfer to an international humanitarian organisation of personal data of a data subject who is physically or legally incapable of giving consent, with a view to accomplishing a task incumbent under the Geneva Conventions or to complying with international humanitarian law applicable in armed conflicts, could be considered to be necessary for an important reason of public interest or because it is in the vital interest of the data subject.
(112) これらの例外は、特に、例えば、公正取引委員会、税務当局又は税関当局の間、金融監督機関の間、並びに、例えば、感染症の接触追跡調査の場合、又は、スポーツにおけるドーピングの抑制及び・又は抑止のた

めに、社会保障に関する事項若しくは公衆衛生について所轄当局の間において行われる国際的なデータ交換の場合など、公益という重要な理由に基づく必要なデータの移転に適用されなければならない。個人データの移転は、データ主体がその同意を与えることができない場合において、身体的な完全性又は生命を含め、データ主体又はそれ以外の者の生命に関する利益のために必須となる利益の保護のために必要となる場合においても、適法とみなされなければならない。十分性認定がない場合、EU 法又は加盟国法は、公共の利益上の重要な理由のために、特別な種類のデータの第三国又は国際機関に対する移転の制限を明確に定めることができる。加盟国は、そのような条項を、欧州委員会に対して通知しなければならない。ジュネーブ諸条約に基づいて行う義務のある職務の遂行という観点から、又は、武力衝突に適用可能な国際人道法を遵守するための、身体的又は法的な原因により同意を与えることができないデータ主体の個人データの国際的な人道組織に対する移転は、公共の利益上の重要な理由のために、又は、データ主体の生命に関する利益に係わるという理由により、必要なものと判断できる。

(113) Transfers which can be qualified as not repetitive and that only concern a limited number of data subjects, could also be possible for the purposes of the compelling legitimate interests pursued by the controller, when those interests are not overridden by the interests or rights and freedoms of the data subject and when the controller has assessed all the circumstances surrounding the data transfer. The controller should give particular consideration to the nature of the personal data, the purpose and duration of the proposed processing operation or operations, as well as the situation in the country of origin, the third country and the country of final destination, and should provide suitable safeguards to protect fundamental rights and freedoms of natural persons with regard to the processing of their personal data. Such transfers should be possible only in residual cases where none of the other grounds for transfer are applicable. For scientific or historical research purposes or statistical purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration. The controller should inform the supervisory authority and the data subject about the transfer.
(113) 管理者の義務的な正当な利益がデータ主体の権利及び自由よりも優先するものではない場合であり、かつ、管理者がその移転に伴う全ての事情を評価している場合、管理者による義務的な正当な利益の目的のために、反復性がないと評価されうるものであり、かつ、限定された人数のデータ主体のみに関する移転を行うことができる。管理者は、特に、個人データの性質、予定されている取扱業務の目的及び期間、並びに、移転元の国、第三国及び最終移転先の国の状況について検討しなければならず、かつ、その個人データの取扱いに関連する自然人の基本的な権利及び自由を保護するための適切な保護措置を提供しなければならない。そのような移転は、移転のための他の適用可能な根拠が存在しない場合においてのみ、これを行うことができる。科学的研究若しくは歴史的研究の目的又は統計の目的に関しては、知識の増加に対する社会の正当な期待を考慮に入れなければならない。管理者は、監督機関及びデータ主体に対し、その移転に関し情報提供しなければならない。

(114) In any case, where the Commission has taken no decision on the adequate level of data protection in a third country, the controller or processor should make use of solutions that provide data subjects with enforceable and effective rights as regards the processing of their data in the Union once those data have been transferred so that that they will continue to benefit from fundamental rights and safeguards.
(114) 欧州委員会が第三国における十分な水準のデータ保護についていかなる決定もしない場合、いかなる場合においても、管理者及び処理者は、データ主体が引き続き基本的な権利及び保護措置を享受するようにするため、データ主体のデータが移転されてしまっても、EU におけるデータ主体のデータの取扱いと関連する執行可能かつ実効的な権利をデータ主体に提供する解決策を、利用できるようにしなければならない。

(115) Some third countries adopt laws, regulations and other legal acts which purport to directly regulate the processing activities of natural and legal persons under the jurisdiction of the Member States. This may include judgments of courts or tribunals or decisions of administrative authorities in third countries requiring a controller or processor to transfer or disclose personal data, and which are not based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State. The extraterritorial application of those laws, regulations and

other legal acts may be in breach of international law and may impede the attainment of the protection of natural persons ensured in the Union by this Regulation. Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met. This may be the case, inter alia, where disclosure is necessary for an important ground of public interest recognised in Union or Member State law to which the controller is subject.
(115) いくつかの第三国は、加盟国の裁判管轄権の下にある自然人及び法人の取扱活動を直接に規律することを旨とする法律、規則及びその他の法的行為を採択している。これは、管理者又は処理者に対して個人データの移転又は開示を求める第三国内の裁判所若しくは法廷の判決又は行政機関の決定であって、司法共助協定のような要求元の第三国とEU若しくは加盟国との間で効力を有する国際協定に基づくものではないものを含みうる。これらの法律、規則及びそれ以外の法的行為の域外適用は、国際法違反となりうるものであり、また、本規則によってEU域内で確保されるべき自然人の保護の達成を害するものとなりうる。移転は、第三国への移転に関して定める本規則の要件に適合する場合にのみ、認められるものとしなければならない。これは、特に、管理者が服するEU法又は加盟国の国内法において認められている公共の利益上の重要な法的根拠のゆえに開示が必要となる場合に該当しうるものである。

(116) When personal data moves across borders outside the Union it may put at increased risk the ability of natural persons to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints. Therefore, there is a need to promote closer cooperation among data protection supervisory authorities to help them exchange information and carry out investigations with their international counterparts. For the purposes of developing international cooperation mechanisms to facilitate and provide international mutual assistance for the enforcement of legislation for the protection of personal data, the Commission and the supervisory authorities should exchange information and cooperate in activities related to the exercise of their powers with competent authorities in third countries, based on reciprocity and in accordance with this Regulation.
(116) 個人データがEUの対外国境を越えて移動する場合、自然人のデータ保護の権利を行使することができること、特に、その情報の違法な利用又は違法な開示から自らを保護することについて、リスクが増大する状況に置かれることとなりうる。それと同時に、監督機関は、その管轄地の域外にある活動に関しては、異議を申立て、又は、調査を行うことができないと結論付けることとなりうる。国境を越えるという文脈の中で、共同で取り組む監督機関の努力は、防止の権限又は救済の権限が不十分であること、一貫性のない法制度、及び、リソースの制約という実務的な障害によっても妨げられうる。それゆえ、監督機関らが国際的な相手と情報交換し、調査を行うことを支援するために、データ保護監督機関の間での緊密な協力を促進する必要がある。個人データ保護のための立法を執行するための国際的な相互支援を促進し、それを提供するための国際協力の仕組みを発展させる目的のために、欧州委員会及び監督機関は、互恵に基づき、かつ、本規則に従って、第三国内の所轄官庁と情報交換をし、又は、それらの機関の権限行使と関連する活動において協力しなければならない。

(117) The establishment of supervisory authorities in Member States, empowered to perform their tasks and exercise their powers with complete independence, is an essential component of the protection of natural persons with regard to the processing of their personal data. Member States should be able to establish more than one supervisory authority, to reflect their constitutional, organisational and administrative structure.
(117) 完全な独立性をもってその職務を遂行し、その権限を行使する地位をもつ加盟国内の監督機関の設置は、自然人の個人データの取扱いと関連する自然人の保護の本質的な構成要素である。加盟国は、その加盟国の国家体制上、国家組織上及び公的組織上の構造の相違に応じて、一又は複数の監督機関を設置できるものとしなければならない。

(118) The independence of supervisory authorities should not mean that the supervisory authorities cannot be subject to control

or monitoring mechanisms regarding their financial expenditure or to judicial review.
(118) 監督機関の独立性は、その財政上の支出に関する管理若しくは監視の仕組み又は司法審査に監督機関が服すことがないということを意味するものではない。

(119) Where a Member State establishes several supervisory authorities, it should establish by law mechanisms for ensuring the effective participation of those supervisory authorities in the consistency mechanism. That Member State should in particular designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the mechanism, to ensure swift and smooth cooperation with other supervisory authorities, the Board and the Commission.
(119) 加盟国が複数の監督機関を設ける場合、その加盟国は、法律によって、一貫性したメカニズムの中におけるそれらの監督機関の効果的な関与を確保するための仕組みを設けなければならない。加盟国は、特に、他の監督機関、委員会及び欧州委員会との迅速かつ円滑な協力関係を確保するため、そのメカニズムへの監督機関らの効果的な関与のための連絡先として機能する監督機関を指定しなければならない。

(120) Each supervisory authority should be provided with the financial and human resources, premises and infrastructure necessary for the effective performance of their tasks, including those related to mutual assistance and cooperation with other supervisory authorities throughout the Union. Each supervisory authority should have a separate, public annual budget, which may be part of the overall state or national budget.
(120) 各監督機関は、EU 全域における他の監督機関との共助及び協力と関連するものを含め、その職務を効果的に遂行するために必要となる資金上及び人員上のリソース、施設及びインフラの提供を受けるものとしなければならない。各監督機関は、独立の公的な予算を受ける。それは、全州の予算又は国内予算の一部とすることができる。

(121) The general conditions for the member or members of the supervisory authority should be laid down by law in each Member State and should in particular provide that those members are to be appointed, by means of a transparent procedure, either by the parliament, government or the head of State of the Member State on the basis of a proposal from the government, a member of the government, the parliament or a chamber of the parliament, or by an independent body entrusted under Member State law. In order to ensure the independence of the supervisory authority, the member or members should act with integrity, refrain from any action that is incompatible with their duties and should not, during their term of office, engage in any incompatible occupation, whether gainful or not. The supervisory authority should have its own staff, chosen by the supervisory authority or an independent body established by Member State law, which should be subject to the exclusive direction of the member or members of the supervisory authority.
(121) 監督機関の構成員に関する一般的な条件は、それぞれの加盟国において法律によって定められなければならず、また、その条件は、特に、透明性のある手続により、政府、政府の構成員、議会若しくは議会の議院、又は、加盟国の国内法に基づいて信任された独立の組織からの提案に基づき、議会、政府又は加盟国の州の長によってその構成員が任命されることを定めなければならない。監督機関の独立性を確保するため、その構成員は、誠実に行動し、その職務と適合しないいかなる行為をも控えなければならず、かつ、その在任中は、報酬の有無を問わず、その職務と適合しない職業に従事してはならない。監督機関は、監督機関によって選任され、又は、加盟国の国内法によって設置される独立の組織によって選任される監督機関自身の職員をもつものとしなければならない。その職員は、その監督機関の構成員の指示のみに従う。

(122) Each supervisory authority should be competent on the territory of its own Member State to exercise the powers and to perform the tasks conferred on it in accordance with this Regulation. This should cover in particular the processing in the context of the activities of an establishment of the controller or processor on the territory of its own Member State, the processing of personal data carried out by public authorities or private bodies acting in the public interest, processing affecting data subjects on its territory or processing carried out by a controller or processor not established in the Union when targeting data subjects residing on its territory. This should include handling complaints lodged by a data subject, conducting

investigations on the application of this Regulation and promoting public awareness of the risks, rules, safeguards and rights in relation to the processing of personal data.
(122) 各監督機関は、その監督機関の加盟国の領土上において、本規則に従ってその監督機関に与えられた権限を行使し、職務を遂行するための職務権限をもつ。これは、特に、その監督機関の加盟国の領土上にある管理者又は処理者の拠点の活動の過程における取扱い、公的機関又は公共の利益において活動をする民間組織によって行われる個人データの取扱い、対象となるデータ主体がその領土上に居住する場合において、EU 域内に拠点のない管理者又は処理者によって行われる、その加盟国上の領土上におけるデータ主体に影響を与える取扱いに対して、適用される。これは、データ主体から申立てられる異議の取り扱い、本規則の適用に関する調査の実施、並びに、個人データの取扱いと関連するリスク、規則、保護措置及び権利についての公衆への周知の促進を含めるものとしなければならない。

(123) The supervisory authorities should monitor the application of the provisions pursuant to this Regulation and contribute to its consistent application throughout the Union, in order to protect natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the internal market. For that purpose, the supervisory authorities should cooperate with each other and with the Commission, without the need for any agreement between Member States on the provision of mutual assistance or on such cooperation.
(123) 監督機関は、自然人の個人データの取扱いに関して自然人を保護し、域内市場内における個人データの自由な移転を促進するために、本規則による条項の適用を監視し、そして、EU 全域におけるその一貫性のある適用に貢献しなければならない。その目的のために、監督機関は、共助の提供又はそのような協力に関する加盟国間の協定を要することなく、相互に協力し、かつ、欧州委員会と協力しなければならない。

(124) Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union and the controller or processor is established in more than one Member State, or where processing taking place in the context of the activities of a single establishment of a controller or processor in the Union substantially affects or is likely to substantially affect data subjects in more than one Member State, the supervisory authority for the main establishment of the controller or processor or for the single establishment of the controller or processor should act as lead authority. It should cooperate with the other authorities concerned, because the controller or processor has an establishment on the territory of their Member State, because data subjects residing on their territory are substantially affected, or because a complaint has been lodged with them. Also where a data subject not residing in that Member State has lodged a complaint, the supervisory authority with which such complaint has been lodged should also be a supervisory authority concerned. Within its tasks to issue guidelines on any question covering the application of this Regulation, the Board should be able to issue guidelines in particular on the criteria to be taken into account in order to ascertain whether the processing in question substantially affects data subjects in more than one Member State and on what constitutes a relevant and reasoned objection.
(124) EU 域内の管理者若しくは処理者の拠点の活動の過程において個人データの取扱いが行われ、かつ、その管理者若しくは処理者が複数の加盟国において拠点がある場合、又は、EU 域内の管理者又は処理者の単一の拠点の活動の過程で行われる取扱いが複数の加盟国内のデータ主体に対して実質的に影響を及ぼす場合、若しくは、実質的に影響を及ぼすおそれがある場合、管理者若しくは処理者の主たる拠点のための監督機関、又は、管理者若しくは処理者の単一の拠点のための監督機関は、主監督機関として行動しなければならない。管理者又は処理者がそれらの加盟国の領土上に拠点をもっていることを理由として、それらの加盟国に居住しているデータ主体が実質的に影響を受けていることを理由に、又は、それらの監督機関に対して異議の申立てがなされたことを理由に、主監督機関は、他の関係監督機関と協力しなければならない。当該加盟国に居住していないデータ主体が異議を申立てた場合、その異議を申立てられた監督機関も、関係監督機関となる。本規則の適用の範囲内にある問題に関するガイドラインを発行する職務の中で、委員会は、特に、当の取扱いが複数の加盟国のデータ主体に対して重大な悪影響を与えるか否か、及び、関連性があり理由を付した異議はどのようなものによって構成されるのかを確認するために考慮に入れられるべき基準に関し、ガイドラインを発行できるものとしなければならない。

(125) The lead authority should be competent to adopt binding decisions regarding measures applying the powers conferred on it in accordance with this Regulation. In its capacity as lead authority, the supervisory authority should closely involve and coordinate the supervisory authorities concerned in the decision-making process. Where the decision is to reject the complaint by the data subject in whole or in part, that decision should be adopted by the supervisory authority with which the complaint has been lodged.
(125) 主監督機関は、本規則に従って監督機関に与えられる権限を適用する措置に関して、拘束力のある決定を採択する職務権限をもつ。その主監督機関としての権限内において、その監督機関は、意思決定の過程において、関係監督機関らと密接に関与し、協力しなければならない。その決定が、データ主体からの異議申立ての全部又は一部を却下するものであるときは、その決定は、その異議申立てを受理した監督機関によって採択されなければならない。

(126) The decision should be agreed jointly by the lead supervisory authority and the supervisory authorities concerned and should be directed towards the main or single establishment of the controller or processor and be binding on the controller and processor. The controller or processor should take the necessary measures to ensure compliance with this Regulation and the implementation of the decision notified by the lead supervisory authority to the main establishment of the controller or processor as regards the processing activities in the Union.
(126) 決定は、主監督機関と関係監督機関との共同で合意されなければならない。その決定は、管理者若しくは処理者の主たる拠点宛て又は単一の拠点宛てのものとし、その管理者及び処理者を拘束するものとしなければならない。管理者又は処理者は、本規則の遵守を確保し、そして、EU 域内における取扱活動に関する管理者又は処理者の主たる拠点に対して主監督機関から通知された決定の実施を確保するために必要となる措置を講じなければならない。

(127) Each supervisory authority not acting as the lead supervisory authority should be competent to handle local cases where the controller or processor is established in more than one Member State, but the subject matter of the specific processing concerns only processing carried out in a single Member State and involves only data subjects in that single Member State, for example, where the subject matter concerns the processing of employees' personal data in the specific employment context of a Member State. In such cases, the supervisory authority should inform the lead supervisory authority without delay about the matter. After being informed, the lead supervisory authority should decide, whether it will handle the case pursuant to the provision on cooperation between the lead supervisory authority and other supervisory authorities concerned (‘one-stop-shop mechanism’), or whether the supervisory authority which informed it should handle the case at local level. When deciding whether it will handle the case, the lead supervisory authority should take into account whether there is an establishment of the controller or processor in the Member State of the supervisory authority which informed it in order to ensure effective enforcement of a decision vis-à-vis the controller or processor. Where the lead supervisory authority decides to handle the case, the supervisory authority which informed it should have the possibility to submit a draft for a decision, of which the lead supervisory authority should take utmost account when preparing its draft decision in that one-stop-shop mechanism.
(127) 主監督機関として行動しない個々の監督機関は、管理者又は処理者が複数の加盟国において拠点を有していても、特定の取扱いの対象が単一の加盟国において行われる取扱いのみと関係するものであり、かつ、当該単一の加盟国内のデータ主体のみを含む場合、例えば、その対象が、ある加盟国の特定の雇用の過程における労働者の個人データの取扱いと関係する場合のような、ローカルな案件を取扱う職務権限をもつ。そのような場合、その監督機関は、主監督機関に対し、遅滞なく、その事柄について通知しなければならない。通知を受けた後、その主監督機関は、主監督機関と他の関係監督機関との間の協力に関する条項によりその案件を取扱うか（以下「ワンストップショップメカニズム」という）、又は、その通知をした監督機関がローカルなレベルでその案件を取扱うべきかについて判断しなければならない。その案件を取扱うか否かを判断する際、その主監督機関は、管理者又は処理者毎の決定の実効的な執行を確保するために、その通知をした監督機関の加盟国内に管理者又は処理者の拠点が存在するか否かを考慮に入れなければならない。その主監督機関がその案件を取扱うと判断するときは、その案件を通知した監督機関は、決定案を送付する機会をもつものとしなければならない。その主監督機関は、当該ワンストップショップメカニズムの中で自らの決定案を準備する際、送付

された決定案を最大限考慮に入れなければならない。

(128) The rules on the lead supervisory authority and the one-stop-shop mechanism should not apply where the processing is carried out by public authorities or private bodies in the public interest. In such cases the only supervisory authority competent to exercise the powers conferred to it in accordance with this Regulation should be the supervisory authority of the Member State where the public authority or private body is established.
(128) 主監督機関に関する規定及びワンストップショップメカニズムに関する規定は、その取扱いが公的機関によって行われる場合、又は、公共の利益において民間組織によって取扱いが行われる場合には、適用されない。そのような場合においては、本規則に従って与えられた権限を行使する職務権限をもつ監督機関のみが、その公的機関又はその民間組織が拠点を有している加盟国の監督機関となるものとしなければならない。

(129) In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have in each Member State the same tasks and effective powers, including powers of investigation, corrective powers and sanctions, and authorisation and advisory powers, in particular in cases of complaints from natural persons, and without prejudice to the powers of prosecutorial authorities under Member State law, to bring infringements of this Regulation to the attention of the judicial authorities and engage in legal proceedings. Such powers should also include the power to impose a temporary or definitive limitation, including a ban, on processing. Member States may specify other tasks related to the protection of personal data under this Regulation. The powers of supervisory authorities should be exercised in accordance with appropriate procedural safeguards set out in Union and Member State law, impartially, fairly and within a reasonable time. In particular each measure should be appropriate, necessary and proportionate in view of ensuring compliance with this Regulation, taking into account the circumstances of each individual case, respect the right of every person to be heard before any individual measure which would affect him or her adversely is taken and avoid superfluous costs and excessive inconveniences for the persons concerned. Investigatory powers as regards access to premises should be exercised in accordance with specific requirements in Member State procedural law, such as the requirement to obtain a prior judicial authorisation. Each legally binding measure of the supervisory authority should be in writing, be clear and unambiguous, indicate the supervisory authority which has issued the measure, the date of issue of the measure, bear the signature of the head, or a member of the supervisory authority authorised by him or her, give the reasons for the measure, and refer to the right of an effective remedy. This should not preclude additional requirements pursuant to Member State procedural law. The adoption of a legally binding decision implies that it may give rise to judicial review in the Member State of the supervisory authority that adopted the decision.
(129) EU 全域における本規則の一貫性のある監視と執行を確保するため、監督機関は、特に、自然人から異議を申立てられた場合において、調査権限、是正権限及び制裁、承認及び助言の権限、並びに、加盟の国内国法に基づく検察当局の権限を妨げることなく、本規則の違反行為に対して司法当局の関心を向けさせること及び訴訟手続を行うことを含め、それぞれの加盟国内において同じ職務及び効果的な権限をもつ。その権限は、禁止を含め、取扱いの一時的又は恒久的な制限を課す権限も含む。加盟国は、本規則に基づく個人データ保護と関連する上記以外の職務を定めることができる。監督機関の権限は、EU 法及び加盟国の国内法に定める適切な手続上の保護措置に従って、公平に、公正に、かつ、合理的な期間内に行使されなければならない。特に、個々の措置は、個々の事案の事情を考慮に入れた上で、本規則の遵守を確保するという観点から適切であり、必要であり、かつ、比例的なものでなければならず、自己に対して不利益な影響を与える個々の措置が講じられる前に全ての者が聴聞を受ける権利を尊重するものであり、かつ、関係者に対する過大な費用負担と過度の不便を避けるものでなければならない。施設へのアクセスと関連する調査権限は、事前に裁判所の承認を得るための要件のような、加盟国の手続法上の特別の要件に従って行使されなければならない。監督機関の個々の法的拘束力のある措置は、書面によるものであり、明確で紛れのないものであり、その措置を発した監督機関、その措置が発せられた日付を表示するものであり、監督機関の長の署名又は当該長によって承認された監督機関の構成員の署名のあるものであり、その措置の理由を提供するものであり、かつ、効果的な司法救済の権利を示すものとしなければならない。このことは、加盟国の手続法による付加的な要件を妨げるものではない。法的拘束力のある決定を採択することは、その決定を採択した監督機関の加盟国において、司法審査の申立て

を提起できることを意味する。

(130) Where the supervisory authority with which the complaint has been lodged is not the lead supervisory authority, the lead supervisory authority should closely cooperate with the supervisory authority with which the complaint has been lodged in accordance with the provisions on cooperation and consistency laid down in this Regulation. In such cases, the lead supervisory authority should, when taking measures intended to produce legal effects, including the imposition of administrative fines, take utmost account of the view of the supervisory authority with which the complaint has been lodged and which should remain competent to carry out any investigation on the territory of its own Member State in liaison with the competent supervisory authority.
(130) 異議を申立てられた監督機関が主監督機関ではない場合、主監督機関は、本規則に定める協力及び一貫性に関する条項に従い、異議を申立てられた監督機関と密接に協力しなければならない。そのような場合、その主監督機関は、制裁金を科すことを含め、法的効果を生じさせる措置を講ずる場合、その異議の申立てを受けた監督機関であり、かつ、職務権限をもつ監督機関と連絡をとりながら自己の加盟国の領土において調査を行う職務権限を維持している監督機関の意見を最大限考慮に入れなければならない。

(131) Where another supervisory authority should act as a lead supervisory authority for the processing activities of the controller or processor but the concrete subject matter of a complaint or the possible infringement concerns only processing activities of the controller or processor in the Member State where the complaint has been lodged or the possible infringement detected and the matter does not substantially affect or is not likely to substantially affect data subjects in other Member States, the supervisory authority receiving a complaint or detecting or being informed otherwise of situations that entail possible infringements of this Regulation should seek an amicable settlement with the controller and, if this proves unsuccessful, exercise its full range of powers. This should include: specific processing carried out in the territory of the Member State of the supervisory authority or with regard to data subjects on the territory of that Member State; processing that is carried out in the context of an offer of goods or services specifically aimed at data subjects in the territory of the Member State of the supervisory authority; or processing that has to be assessed taking into account relevant legal obligations under Member State law.
(131) 管理者又は処理者の取扱活動に関して別の監督機関が主監督機関として行動しなければならないけれども、異議の具体的な事項又は関係する違反行為のおそれが、異議の申し立てられた加盟国の管理者又は処理者の取扱いのみに関係するものである場合、又は、検出された違反行為のおそれ及びその事項が、別の加盟国のデータ主体に対して重大な影響を及ぼしておらず、又は、そのおそれがない場合、異議を受理した監督機関、又は、本規則の違反行為の可能性を伴う状況を検知し、若しくは、別途情報提供を受けている監督機関は、管理者との友好的な解決を模索しなければならず、そして、そのような解決ができないときは、監督機関の権限を全面的に行使しなければならない。このことは、その監督機関の加盟国の領土内で行われる特定の取扱い、又は、当該加盟国の領土内のデータ主体と関連する特定の取扱い；その監督機関の加盟国の領土内のデータ主体を特に対象とする物品又はサービスの提供の過程で行われる取扱い；又は、加盟国の国内法に基づく関連する法的義務を考慮に入れて評価されなければならない取扱いを含めるものとしなければならない。

(132) Awareness-raising activities by supervisory authorities addressed to the public should include specific measures directed at controllers and processors, including micro, small and medium-sized enterprises, as well as natural persons in particular in the educational context.
(132) 監督機関による公衆向けの周知活動は、中小零細企業、並びに、特に教育の過程における自然人を含め、管理者及び処理者向けの具体的な措置を含めるものとしなければならない。

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

(133) 監督機関は、域内市場において本規則の一貫性のある適用及び執行を確保するために、その職務の遂行において相互に支援し、また、共助を提供しなければならない。共助を要求する監督機関は、共助の要求に対して当該別の監督機関が当該要求を受領した後 1 か月以内に、何らの回答も受けない場合、暫定的な措置を採択できる。

(134) Each supervisory authority should, where appropriate, participate in joint operations with other supervisory authorities. The requested supervisory authority should be obliged to respond to the request within a specified time period.
(134) 個々の監督機関は、それが適切なときは、他の監督機関との共同の職務遂行に参加しなければならない。要求を受けた監督機関は、指定された期限内に、その要求に対する回答を義務付けられるものとする。

(135) In order to ensure the consistent application of this Regulation throughout the Union, a consistency mechanism for cooperation between the supervisory authorities should be established. That mechanism should in particular apply where a supervisory authority intends to adopt a measure intended to produce legal effects as regards processing operations which substantially affect a significant number of data subjects in several Member States. It should also apply where any supervisory authority concerned or the Commission requests that such matter should be handled in the consistency mechanism. That mechanism should be without prejudice to any measures that the Commission may take in the exercise of its powers under the Treaties.
(135) EU 全域における本規則の一貫性のある適用を確保するため、監督機関の間の協力のための一貫性メカニズムが構築されなければならない。特に、複数の加盟国内の大勢のデータ主体に対して重大な影響を及ぼす取扱業務に関し、法的効果を生じさせる措置を監督機関が採択しようとする場合に、このメカニズムは適用されなければならない。関係監督機関又は欧州委員会が、そのような事柄は一貫性メカニズムの中で取り扱われるべきであると要求する場合においても、適用されなければならない。そのメカニズムは、欧州委員会が諸条約に基づく権限を行使する際に講ずることのできる措置を妨げないものとする。

(136) In applying the consistency mechanism, the Board should, within a determined period of time, issue an opinion, if a majority of its members so decides or if so requested by any supervisory authority concerned or the Commission. The Board should also be empowered to adopt legally binding decisions where there are disputes between supervisory authorities. For that purpose, it should issue, in principle by a two-thirds majority of its members, legally binding decisions in clearly specified cases where there are conflicting views among supervisory authorities, in particular in the cooperation mechanism between the lead supervisory authority and supervisory authorities concerned on the merits of the case, in particular whether there is an infringement of this Regulation.
(136) 一貫性メカニズムを適用する際、欧州データ保護会議は、欧州データ保護会議の構成員の多数が決定した場合、又は、関係監督機関若しくは欧州委員会からそのように要求された場合、定められた期間内に、その意見を発しなければならない。監督機関の間で見解の対立がある場合、欧州データ保護会議は、法的拘束力のある決定を採択する権限も与えられなければならない。その目的のために、欧州データ保護会議は、監督機関の間において見解の対立があることが明確に示されている案件、特に、協力のメカニズムの中で主監督機関と関係監督機関との間でその案件の結論について対立がある場合、さらに本規則の違反行為があるか否かについて対立がある場合において、原則として、その構成員の 3 分の 2 の多数決により、法的拘束力のある決定をしなければならない。

(137) There may be an urgent need to act in order to protect the rights and freedoms of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded. A supervisory authority should therefore be able to adopt duly justified provisional measures on its territory with a specified period of validity which should not exceed three months.
(137) 特に、データ主体の権利の行使が深刻に害されうるような危険が存在する場合において、データ主体の権利及び自由を保護するために行動する緊急の必要がありうる。それゆえ、監督機関は、その監督機関の領土

内において、3 か月を超えない特定の有効期間を持つ、正当な根拠をもつ暫定的な措置を採択できるものとしなければならない。

(138) The application of such mechanism should be a condition for the lawfulness of a measure intended to produce legal effects by a supervisory authority in those cases where its application is mandatory. In other cases of cross-border relevance, the cooperation mechanism between the lead supervisory authority and supervisory authorities concerned should be applied and mutual assistance and joint operations might be carried out between the supervisory authorities concerned on a bilateral or multilateral basis without triggering the consistency mechanism.
(138) このようなメカニズムを適用することは、その適用が義務となる場合においては、監督機関によって法的効果を生じさせる措置の適法性の条件になるものとする。これ以外の国境を越える関連案件に関しては、主監督機関と関係監督機関との間の協力のメカニズムが適用されなければならず、また、一貫性メカニズムを発動させることなく、二国間又は多国間で、関係監督機関の間において、共助及び共同の職務遂行が行われうる。

(139) In order to promote the consistent application of this Regulation, the Board should be set up as an independent body of the Union. To fulfil its objectives, the Board should have legal personality. The Board should be represented by its Chair. It should replace the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data established by Directive 95/46/EC. It should consist of the head of a supervisory authority of each Member State and the European Data Protection Supervisor or their respective representatives. The Commission should participate in the Board's activities without voting rights and the European Data Protection Supervisor should have specific voting rights. The Board should contribute to the consistent application of this Regulation throughout the Union, including by advising the Commission, in particular on the level of protection in third countries or international organisations, and promoting cooperation of the supervisory authorities throughout the Union. The Board should act independently when performing its tasks.
(139) 本規則の一貫性のある適用を促進するため、欧州データ保護会議は、EU の独立の組織として設置されなければならない。この目的を充足するために、欧州データ保護会議は、法人格をもつものとしなければならない。欧州データ保護会議は、その議長によって代表される。欧州データ保護会議は、指令 95/46/EC によって設置された個人データの保護と関連する個人の保護に関する作業部会（the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data）と置き換わるものとしなければならない。欧州データ保護会議は、それぞれの加盟国の監督機関の長及び欧州データ保護監督機関又はそれらの個々の代表者によって構成されるものとしなければならない。欧州委員会は、議決権なく委員会の活動に参加するものとし、また、欧州データ保護監督機関は、特定の議決権をもつものとしなければならない。欧州データ保護会議は、特に、第三国又は国際機関における保護のレベルに関して欧州委員会に助言すること、及び、EU 全域における監督機関の協力を促進すること等を通じて、EU 全域における本規則の一貫性のある適用のために貢献しなければならない。欧州データ保護会議は、その職務を遂行する際、独立して行動しなければならない。

(140) The Board should be assisted by a secretariat provided by the European Data Protection Supervisor. The staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation should perform its tasks exclusively under the instructions of, and report to, the Chair of the Board.
(140) 欧州データ保護会議は、欧州データ保護監督機関から提供される事務局によって補佐されるものとする。本規則によって欧州データ保護会議の権限とされる職務に関与する欧州データ保護監督機関の職員は、保護会議の議長の指示の下においてのみその職務を遂行し、かつ、その議長に直属する。

(141) Every data subject should have the right to lodge a complaint with a single supervisory authority, in particular in the Member State of his or her habitual residence, and the right to an effective judicial remedy in accordance with Article 47 of the Charter if the data subject considers that his or her rights under this Regulation are infringed or where the supervisory authority does not act on a complaint, partially or wholly rejects or dismisses a complaint or does not act where such action is necessary to protect the rights of the data subject. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject

of the progress and the outcome of the complaint within a reasonable period. If the case requires further investigation or coordination with another supervisory authority, intermediate information should be given to the data subject. In order to facilitate the submission of complaints, each supervisory authority should take measures such as providing a complaint submission form which can also be completed electronically, without excluding other means of communication.
(141) 全てのデータ主体は、特に、当該データ主体の定居住地の加盟国において、単一の監督機関に異議を申立てる権利をもち、かつ、本規則に基づく自己の権利が侵害されたと判断する場合、又は、監督機関がデータ主体の権利を保護するために必要である場合にその異議の全部又は一部を棄却若しくは却下し何ら行動しない場合、憲章の第 47 条に従い、効果的な司法救済を受ける権利を有するものとしなければならない。異議申立て後の調査は、司法審査に服するものとして、特定の案件において適切な範囲内で行われなければならない。監督機関は、データ主体に対し、合理的な期間内に、その異議の進捗状況及び結果について、情報提供しなければならない。更なる調査又は別の監督機関との連携が必要となる場合、データ主体に対し、中間的な情報提供が行われなければならない。異議の申立てを容易にするために、各監督機関は、他の通信手段を排除することなく、電子的に完結できる異議申立ての方式を提供するといったような措置を講じなければならない。

(142) Where a data subject considers that his or her rights under this Regulation are infringed, he or she should have the right to mandate a not-for-profit body, organisation or association which is constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest and is active in the field of the protection of personal data to lodge a complaint on his or her behalf with a supervisory authority, exercise the right to a judicial remedy on behalf of data subjects or, if provided for in Member State law, exercise the right to receive compensation on behalf of data subjects. A Member State may provide for such a body, organisation or association to have the right to lodge a complaint in that Member State, independently of a data subject's mandate, and the right to an effective judicial remedy where it has reasons to consider that the rights of a data subject have been infringed as a result of the processing of personal data which infringes this Regulation. That body, organisation or association may not be allowed to claim compensation on a data subject's behalf independently of the data subject's mandate.
(142) データ主体が、本規則に基づく自己の権利が侵害されていると考える場合、当該データ主体は、加盟国の国内法に従って組織され、公共の利益に属する制定法上の目的をもち、かつ、データ主体の代わりとなって監督機関に異議の申立てをし、データ主体の代わりとなって司法救済の権利を行使し、又は、加盟国が定めている場合には、データ主体の代わりとなって損害賠償金を受領する権利を行使するために、個人データの保護の領域において活動する非営利の組織、団体又は協会に対し、委任する権利を有するものとしなければならない。加盟国は、データ主体の委任を受けることなく、そのような組織、団体又は協会が当該加盟国において異議を申し立てる権利、及び、それらの組織が、本規則に違反する個人データの取扱いの結果としてデータ主体の権利が侵害されていると判断すべき根拠をもつ場合における効果的な司法救済の権利を定めることができる。その組織、団体又は協会は、データ主体の委任を受けることなく、データ主体の代わりに損害賠償を請求することは認められない。

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

and should be conducted in accordance with that Member State's procedural law. Those courts should exercise full jurisdiction, which should include jurisdiction to examine all questions of fact and law relevant to the dispute before them.
Where a complaint has been rejected or dismissed by a supervisory authority, the complainant may bring proceedings before the courts in the same Member State. In the context of judicial remedies relating to the application of this Regulation, national courts which consider a decision on the question necessary to enable them to give judgment, may, or in the case provided for in Article 267 TFEU, must, request the Court of Justice to give a preliminary ruling on the interpretation of Union law, including this Regulation. Furthermore, where a decision of a supervisory authority implementing a decision of the Board is challenged before a national court and the validity of the decision of the Board is at issue, that national court does not have the power to declare the Board's decision invalid but must refer the question of validity to the Court of Justice in accordance with Article 267 TFEU as interpreted by the Court of Justice, where it considers the decision invalid. However, a national court may not refer a question on the validity of the decision of the Board at the request of a natural or legal person which had the opportunity to bring an action for annulment of that decision, in particular if it was directly and individually concerned by that decision, but had not done so within the period laid down in Article 263 TFEU.
(143) 自然人又は法人は、TFEU の第 263 条に定める条件の下で、欧州司法裁判所において、欧州データ保護会議の決定の取消しを求める訴えを提起する権利を有する。その決定の名宛人として、その決定に対して不服申立てをする意思のある関係監督機関は、TFEU の第 263 条に従い、その決定が通知された後 2 か月以内に訴えを提起しなければならない。欧州データ保護会議の決定が、管理者、処理者又は異議申立人に対する直接的かつ個別的な決定である場合、それらの者は、TFEU の第 263 条に従い、欧州データ保護会議の Web サイト上でその決定が公示された時から 2 か月以内に、その決定の取消しを求める訴えを提起することができる。TFEU の第 263 条に基づくこの権利を妨げることなく、個々の自然人又は法人は、それらの者に関して法的効果を発生させる監督機関の決定を不服として、職務権限をもつ自国の裁判所において、効果的な司法救済を得るものとしなければならない。当該決定は、特に、監督機関による調査権限、是正権限及び承認権限と関係するもの、又は、異議の棄却若しくは却下に関するものである。ただし、この効果的な司法救済の権利は、監督機関から発された意見や提供された助言のような、監督機関によって講じられた法的拘束力のない措置については、適用対象外となる。監督機関に対する訴訟手続は、その監督機関が設けられている加盟国の裁判所において提起されなければならず、かつ、当該加盟国の手続法に従って行われなければならない。これらの裁判所は、裁判管轄権を全面的に行使しなければならず、その管轄権は、その裁判所に提起された紛争と関係する全ての事実上の争点及び法律上の争点を審理するための裁判管轄権を含むものとしなければならない。
異議申立てが監督機関によって却下又は棄却された場合、その異議申立人は、同じ加盟国内の裁判所において、訴訟を提起できる。本規則の適用と関係する司法救済の過程においては、その事件について判決を与えることを可能とするために必要な争点の判断をする国内裁判所は、欧州司法裁判所に対し、本規則を含め、EU 法の解釈に関する先決裁定を与えることを求めることができ、TFEU の第 267 条に規定する場合には、そのように求めなければならない。さらに、欧州データ保護会議の決定を踏まえている監督機関の決定に対して国内裁判所において不服申立てがなされ、かつ、その欧州データ保護会議の決定の有効性が争点となっている場合、当該国内裁判所は、その欧州データ保護会議の決定を無効であると宣言する権限をもたず、その国内裁判所がその決定を無効であると判断するときは、欧州司法裁判所によって解釈されるものとしての TFEU の第 267 条に従い、その有効性に関する争点の判断を欧州司法裁判所に照会しなければならない。ただし、国内裁判所は、特に、それが当該決定によって直接的かつ個別に関係するものであっても、TFEU の第 263 条に定める期間内にその申立てがなされたものではない場合、その決定の取消しを求める訴訟を提起する機会をもっていた自然人又は法人の求めに対し、当該欧州データ保護会議の決定の有効性に関する争点の判断の照会をしてはならない。

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

jurisdiction in favour of the court first seized if that court has jurisdiction over the proceedings in question and its law permits the consolidation of such related proceedings. Proceedings are deemed to be related where they are so closely connected that it is expedient to hear and determine them together in order to avoid the risk of irreconcilable judgments resulting from separate proceedings.
(144) 監督機関の決定を不服とする訴訟の提起を受けた裁判所が、同じ管理者又は処理者による取扱いについて同じ対象である場合のような、同じ取扱いと関係する訴訟手続、又は、同じ訴訟原因による訴訟手続が、他の加盟国の管轄権をもつ裁判所に提起されていると信ずべき根拠をもつときは、その裁判所は、そのような関連訴訟の存在を確認するために当該裁判所と連絡をとらなければならない。関連訴訟手続が他の加盟国の裁判所に係属しているときは、最初に訴訟係属した裁判所以外の裁判所は、その訴訟手続の進行を停止することができ、また、最初に訴訟係属した裁判所が当の訴訟手続について管轄権をもち、かつ、その加盟国の国内法がそのような関連訴訟事件の併合を認めている場合、どちらか一方の訴訟当事者からの求めにより、最初に訴訟係属した裁判所の管轄権を優先させることができる。別の訴訟手続から相反する内容の判決が生ずるリスクを避けるため、異なる訴訟手続が密接に関係しており、それらについて一緒に審理し判断したほうが得策である場合には、それらの訴訟手続は、関連するものとみなされる。

(145) For proceedings against a controller or processor, the plaintiff should have the choice to bring the action before the courts of the Member States where the controller or processor has an establishment or where the data subject resides, unless the controller is a public authority of a Member State acting in the exercise of its public powers.
(145) 管理者又は処理者を相手方とする訴訟手続に関し、管理者がその公権力の行使において行動する加盟国の行政機関である場合を除き、原告は、管理者又は処理者がその拠点をもつ加盟国の裁判所、又は、データ主体の居住地である加盟国の裁判所において、訴えを提起する選択肢をもつものとしなければならない。

(146) The controller or processor should compensate any damage which a person may suffer as a result of processing that infringes this Regulation. The controller or processor should be exempt from liability if it proves that it is not in any way responsible for the damage. The concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation. This is without prejudice to any claims for damage deriving from the violation of other rules in Union or Member State law. Processing that infringes this Regulation also includes processing that infringes delegated and implementing acts adopted in accordance with this Regulation and Member State law specifying rules of this Regulation. Data subjects should receive full and effective compensation for the damage they have suffered. Where controllers or processors are involved in the same processing, each controller or processor should be held liable for the entire damage. However, where they are joined to the same judicial proceedings, in accordance with Member State law, compensation may be apportioned according to the responsibility of each controller or processor for the damage caused by the processing, provided that full and effective compensation of the data subject who suffered the damage is ensured. Any controller or processor which has paid full compensation may subsequently institute recourse proceedings against other controllers or processors involved in the same processing.
(146) 管理者又は処理者は、本規則に違反する取扱いの結果として人が被るであろう損害の賠償をしなければならない。管理者又は処理者は、その損害に関しいかなる態様の責任もないことを証明したときは、その法的責任を免れる。損害の概念は、本規則の目的を完全に反映する態様で、欧州司法裁判所の判例法に照らし、幅広く解釈されなければならない。これは、EU 法又は加盟国の国内法中の他の規定の違反から生ずる損害に関するいかなる訴訟をも妨げるものではない。本規則に違反する取扱いは、本規則及び本規則の細則を定める加盟国の国内法に従って採択される委任される行為及び実装行為に違反する取扱いも含む。データ主体は、自らが被った損害について、完全かつ効果的な損害賠償を受けるものとする。管理者又は処理者が同じ取扱いに関与する場合、個々の管理者又は処理者は、損害の全部について法的責任を負わなければならない。ただし、それらの者が同じ訴訟手続に加わっている場合、被害を受けたデータ主体の完全かつ効果的な損害賠償が確保される限り、加盟国の国内法に従い、その取扱いから生じた損害について、個々の管理者又は処理者の責任の割合に応じた賠償とすることができる。全額を弁償した管理者又は処理者は、その後に、同じ取扱いに関与した他の管理者又は処理者を相手方として、求償請求の訴えを提起できる。

(147) Where specific rules on jurisdiction are contained in this Regulation, in particular as regards proceedings seeking a judicial remedy including compensation, against a controller or processor, general jurisdiction rules such as those of Regulation (EU) No 1215/2012 of the European Parliament and of the Council [13] should not prejudice the application of such specific rules.
(147) 特に、損害賠償を含め、管理者又は処理者を相手方として司法救済を求める訴訟手続に関し、裁判管轄権に関する特別規定が本規則の中に含まれている場合、欧州議会及び理事会の規則(EU) No 1215/2012[13]中の規定のような裁判管轄権に関する一般的な規定は、そのような特別規定の適用を妨げてはならない。

(148) In order to strengthen the enforcement of the rules of this Regulation, penalties including administrative fines should be imposed for any infringement of this Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation. In a case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine. Due regard should however be given to the nature, gravity and duration of the infringement, the intentional character of the infringement, actions taken to mitigate the damage suffered, degree of responsibility or any relevant previous infringements, the manner in which the infringement became known to the supervisory authority, compliance with measures ordered against the controller or processor, adherence to a code of conduct and any other aggravating or mitigating factor. The imposition of penalties including administrative fines should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter, including effective judicial protection and due process.
(148) 本規則の規定の執行を強化するために、本規則により監督機関によって課される適切な措置に加え、又は、これに代えて、本規則の違反行為に対し、制裁金を含め、制裁が加えられなければならない。軽微な違反行為の場合、又は、課される制裁金が自然人に対して過大な負担を構成するような場合、制裁金の代わりに注意処分を行うことができる。ただし、その違反行為の性質、重大性及び持続期間、その違反行為が意図的なものであること、被った損害を軽減させるために講じられた行動、責任の程度及び関連する過去の違反行為、その違反行為がどのようにして監督機関に認知されることになったのか、管理者又は処理者に対して命じられた措置の遵守、行動準則の遵守、並びに、これら以外の加重要素及び軽減要素を適正に考慮しなければならない。制裁金を含め、制裁の実施は、効果的な司法上の保護及び適正手続を含め、EU 法及び憲章の一般的な基本原則に従う適切な手続上の保護措置に服するものとしなければならない。

(149) Member States should be able to lay down the rules on criminal penalties for infringements of this Regulation, including for infringements of national rules adopted pursuant to and within the limits of this Regulation. Those criminal penalties may also allow for the deprivation of the profits obtained through infringements of this Regulation. However, the imposition of criminal penalties for infringements of such national rules and of administrative penalties should not lead to a breach of the principle of ne bis in idem, as interpreted by the Court of Justice.
(149) 加盟国は、本規則に従い、かつ、本規則の制限の範囲内で採択された国内規定の違反行為に関するものを含め、本規則の違反行為に対する刑事罰に関する規定を定めることができる。その刑事罰は、本規則の違反行為によって得られた利益の没収を認めることもできる。ただし、そのような国内規定の違反行為に対して刑罰及び行政上の制裁を加えることが、欧州司法裁判所によって解釈されるものとしての一事不再理の原則を侵害するような結果を導いてはならない。

(150) In order to strengthen and harmonise administrative penalties for infringements of this Regulation, each supervisory authority should have the power to impose administrative fines. This Regulation should indicate infringements and the upper limit and criteria for setting the related administrative fines, which should be determined by the competent supervisory

[13] Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (OJ L 351, 20.12.2012, p. 1).
裁判管轄権並びに民事及び商事における判決の承認及び執行に関する欧州議会及び理事会の 2012 年 12 月 12 日の規則(EU) No 1215/2012（OJ L 351, 20.12.2012, p.1）

authority in each individual case, taking into account all relevant circumstances of the specific situation, with due regard in particular to the nature, gravity and duration of the infringement and of its consequences and the measures taken to ensure compliance with the obligations under this Regulation and to prevent or mitigate the consequences of the infringement. Where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes. Where administrative fines are imposed on persons that are not an undertaking, the supervisory authority should take account of the general level of income in the Member State as well as the economic situation of the person in considering the appropriate amount of the fine. The consistency mechanism may also be used to promote a consistent application of administrative fines. It should be for the Member States to determine whether and to which extent public authorities should be subject to administrative fines. Imposing an administrative fine or giving a warning does not affect the application of other powers of the supervisory authorities or of other penalties under this Regulation.
(150) 本規則の違反行為に対する行政上の制裁を強化し、整合性のとれたものとするため、各監督機関は、制裁金を加える権限をもつものとしなければならない。本規則は、関連する制裁金を決定するための違反行為、上限及び基準を示すものとしなければならならず、それは、個々の事案において、監督機関によって、特定の状況における全ての関連する事情を考慮に入れた上で、特に、違反行為の性質、重大性及び持続期間、その結果として発生した事態、並びに、本規則に基づく義務の遵守を確保し、違反行為による結果の発生を防止又は軽減するために講じられた措置を適切に考慮した上で、決定されなければならない。制裁金が事業者に対して加えられる場合、その目的との関係においては、事業者とは、TFEU の第 101 条及び第 102 条に従った事業者として理解されなければならない。制裁金が事業者ではない者に対して加えられる場合、監督機関は、制裁金の適切な金額を検討するに際し、その加盟国における一般的な所得レベル及び当該の者の経済状態を考慮に入れなければならない。一貫性メカニズムは、制裁金の一貫性のある適用を促進するためにも用いることができる。行政機関が制裁金に服すべきか否か及びその範囲は、加盟国によって定められなければならない。制裁金を加えること、又は、警告を与えることは、本規則に基づく監督機関のそれ以外の権限の行使又はそれ以外の制裁の適用に影響を及ぼすものではない。

(151) The legal systems of Denmark and Estonia do not allow for administrative fines as set out in this Regulation. The rules on administrative fines may be applied in such a manner that in Denmark the fine is imposed by competent national courts as a criminal penalty and in Estonia the fine is imposed by the supervisory authority in the framework of a misdemeanour procedure, provided that such an application of the rules in those Member States has an equivalent effect to administrative fines imposed by supervisory authorities. Therefore the competent national courts should take into account the recommendation by the supervisory authority initiating the fine. In any event, the fines imposed should be effective, proportionate and dissuasive.
(151) デンマーク及びエストニアの法制度は、本規則に定める制裁金を認めていない。デンマークにおいては、職務権限をもつ国内裁判所によって刑罰として制裁金が科されるものとし、そして、エストニアにおいては、監督機関によって微罪の手続の枠組みの中で制裁金が科されるものとするという方法で、制裁金に関する法令を適用できるが、これらの加盟国におけるそのような法令の適用が監督機関によって加えられる制裁金と均等の効果をもつ事が条件となる。それゆえ、職務権限をもつ国内裁判所は、制裁金を求める監督機関からの勧告を考慮に入れなければならない。いずれの場合においても、制裁金は、効果的であり、比例的であり、かつ、抑止力のあるものでなければならない。

(152) Where this Regulation does not harmonise administrative penalties or where necessary in other cases, for example in cases of serious infringements of this Regulation, Member States should implement a system which provides for effective, proportionate and dissuasive penalties. The nature of such penalties, criminal or administrative, should be determined by Member State law.
(152) 本規則が行政上の制裁と整合しない場合、又は、例えば、本規則の重大な違反行為の場合のような、それ以外の場合にその必要性がある場合は、加盟国は、効果的であり、比例的であり、かつ、抑止力のある処罰を定める法制度を実装しなければならない。そのような制裁の法的性質、刑事罰とするか制裁金とするかは、加盟国の国内法によって定められるものとしなければならない。

(153) Member States law should reconcile the rules governing freedom of expression and information, including journalistic, academic, artistic and or literary expression with the right to the protection of personal data pursuant to this Regulation. The processing of personal data solely for journalistic purposes, or for the purposes of academic, artistic or literary expression should be subject to derogations or exemptions from certain provisions of this Regulation if necessary to reconcile the right to the protection of personal data with the right to freedom of expression and information, as enshrined in Article 11 of the Charter. This should apply in particular to the processing of personal data in the audiovisual field and in news archives and press libraries. Therefore, Member States should adopt legislative measures which lay down the exemptions and derogations necessary for the purpose of balancing those fundamental rights. Member States should adopt such exemptions and derogations on general principles, the rights of the data subject, the controller and the processor, the transfer of personal data to third countries or international organisations, the independent supervisory authorities, cooperation and consistency, and specific data-processing situations. Where such exemptions or derogations differ from one Member State to another, the law of the Member State to which the controller is subject should apply. In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly.
(153) 加盟国の国内法は、報道、学問上、芸術又は文学上の表現を含め、表現及び情報伝達の自由を規律する規定と、本規則による個人データの保護の権利との間の調和を図らなければならない。報道の目的のため、又は、学問上、芸術若しくは文学上の表現の目的のためにのみ行われる個人データの取扱いは、個人データの保護に関する権利と憲章の第 11 条に掲げられている表現及び情報伝達の自由の権利とを調和させる必要があるときは、本規則の一定の条項からの特例又は例外の対象になるものとする。このことは、特に、視聴覚の分野並びにニュース保管及び報道ライブラリにおける個人データの取扱いに関して適用されなければならない。それゆえ、加盟国は、これらの基本的な諸権利の間のバランスをとる目的のために必要な例外条項及び特例条項を定める立法上の措置を講じなければならない。加盟国は、一般的な基本原則、データ主体の権利、管理者及び処理者、第三国又は国際機関に対する個人データの移転、独立の監督機関、協力と一貫性、並びに、特別のデータの取扱いに関し、そのような例外条項及び特例条項を採択しなければならない。そのような例外条項又は特例条項が加盟国間で区々になっている場合、管理者が服する加盟国の法律が適用される。全ての民主主義社会における表現の自由の権利の重要性を考慮に入れるため、報道のような、表現の自由と関連する諸概念を広く解釈する必要がある。

(154) This Regulation allows the principle of public access to official documents to be taken into account when applying this Regulation. Public access to official documents may be considered to be in the public interest. Personal data in documents held by a public authority or a public body should be able to be publicly disclosed by that authority or body if the disclosure is provided for by Union or Member State law to which the public authority or public body is subject. Such laws should reconcile public access to official documents and the reuse of public sector information with the right to the protection of personal data and may therefore provide for the necessary reconciliation with the right to the protection of personal data pursuant to this Regulation. The reference to public authorities and bodies should in that context include all authorities or other bodies covered by Member State law on public access to documents. Directive 2003/98/EC of the European Parliament and of the Council [14] leaves intact and in no way affects the level of protection of natural persons with regard to the processing of personal data under the provisions of Union and Member State law, and in particular does not alter the obligations and rights set out in this Regulation. In particular, that Directive should not apply to documents to which access is excluded or restricted by virtue of the access regimes on the grounds of protection of personal data, and parts of documents accessible by virtue of those regimes which contain personal data the re-use of which has been provided for by law as being incompatible with the law concerning the protection of natural persons with regard to the processing of personal data.
(154) 本規則は、本規則の適用の際に考慮されるべき、公文書への公衆のアクセスの原則を認める。公文書への公衆のアクセスは、公共の利益に属するものと考えることができる。公的機関又は公的組織によって保有される文書中の個人データは、その公的機関又は公的組織が服する EU 法又は加盟国の国内法によってその開示が定められている場合、その公的機関又は公的組織によって公衆に開示されうるものとしなければならない。

そのような法律は、公文書への公衆のアクセス及び公的分野にある情報の再利用と個人データの保護の権利との調和を図るものとしなければならず、また、それゆえ、本規則による個人データの保護の権利との必要な調和を図ることを定めることができる。公的機関及び公的組織に対する照会は、その文脈において、文書への公衆のアクセスに関する加盟国の国内法の適用範囲内にある全ての機関及びそれ以外の組織を含むものとしなければならない。欧州議会及び理事会の指令 2003/98/EC[14]は、そのまま維持されており、そして、EU 法又は加盟国の国内法の条項に基づく個人データの取扱いと関連する自然人の保護のレベルに対して、いかなる方法においても影響を与えることがなく、また、特に、本規則に定める義務及び権利を変更するものではない。特に、同指令は、個人データの保護を根拠とするアクセス制度によりアクセスが禁止又は制限されている文書、及び、その制度により部分的に公開可能な文書であっても、当該部分に個人データを含み、その部分の二次利用が個人データの取扱いと関連する自然人の保護に関する法律と適合しないものとして、当該法律によって定められているものには適用されない。

(155) Member State law or collective agreements, including 'works agreements', may provide for specific rules on the processing of employees' personal data in the employment context, in particular for the conditions under which personal data in the employment context may be processed on the basis of the consent of the employee, the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.
(155) 加盟国の国内法、又は、「労働協約」を含む協約は、雇用の過程における労働者の個人データの取扱いに関して、特に、雇用の過程において、労働者の同意に基づき、求人、法律又は協約に定める就労義務の履行を含む雇用契約の履行、仕事の管理、企画及び編成、職場における平等と多様性、職場における健康と安全の目的、及び、個人ベース及び集団ベースで、雇用と関連する権利の行使及び利益の享受の目的、並びに、雇用関係の終了の目的のために個人データを取扱うことができる場合の条件に関して、その特別規定を定めることができる。

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

[14] Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information (OJ L 345, 31.12.2003, p. 90).
公的部門の情報の二次利用に関する欧州議会及び理事会の 2003 年 11 月 17 日の指令 2003/98/EC （OJ L 345, 31.12.2003, p. 90）

(156) 公共の利益における保管の目的、科学的研究若しくは歴史的研究の目的又は統計の目的のための個人データの取扱いは、本規則により、データ主体の権利及び自由のための適切な保護措置に服するものとしなければならない。それらの保護措置は、特に、データの最小化の原則を確保するために、技術上及び組織上の措置が設けられることを確保しなければならない。公共の利益における保管の目的、科学的研究若しくは歴史的研究の目的又は統計の目的のための個人データの追加的な取扱いは、（例えば、データの仮名化のような）適切な保護措置が存在することを条件として、データ主体の識別を許さない、若しくは、許さなくなったデータの取扱いによってその目的を充足させることができるということを管理者が評価したときに、行われるべきである。加盟国は、公共の利益における保管の目的、科学的研究若しくは歴史的研究の目的又は統計の目的のために行われる個人データの取扱いのための適切な保護措置を定めなければならない。加盟国は、公共の利益における保管の目的、科学的研究若しくは歴史的研究の目的又は統計の目的のために個人データの取扱いが行われる場合、特別の条件の下で、かつ、データ主体のための適切な保護措置の下、情報提供義務、並びに、訂正の権利、削除の権利、忘れられる権利、取扱いの制限の権利、データポータビリティの権利及び異議を述べる権利に関し、その細則及び特例を定めることが認められる。当該条件及び保護措置は、データ主体がそれらの権利を行使するための特別の手続を伴うものとすることができるが、これは比例性原則及び必要性原則に従って個人データの取扱いを最小化することを狙いとする技術上及び組織上の措置に沿う特別の取扱いによって求められる目的に照らして適切であることが条件となる。また、科学的研究の目的のための個人データの取扱いは、臨床試験に関する法令のような、関連する他の立法を遵守しなければならない。

(157) By coupling information from registries, researchers can obtain new knowledge of great value with regard to widespread medical conditions such as cardiovascular disease, cancer and depression. On the basis of registries, research results can be enhanced, as they draw on a larger population. Within social science, research on the basis of registries enables researchers to obtain essential knowledge about the long-term correlation of a number of social conditions such as unemployment and education with other life conditions. Research results obtained through registries provide solid, high-quality knowledge which can provide the basis for the formulation and implementation of knowledge-based policy, improve the quality of life for a number of people and improve the efficiency of social services. In order to facilitate scientific research, personal data can be processed for scientific research purposes, subject to appropriate conditions and safeguards set out in Union or Member State law.
(157) 登録所からの情報と連結することによって、研究者は、心血管疾患、ガン及びうつ病のような広い範囲の健康状態と関連する大きな価値のある新たな知識を得ることができる。登録所を基盤として、その研究結果は、より大きな人口に基づいて考察することにより、深めることができる。社会科学の範囲内では、登録所に基づく調査は、失業及び教育のような、多数の社会条件とそれ以外の生活条件との長期間にわたる相関関係に関する基礎的な知識を研究者が得ることを可能にする。登録所から得られる調査結果は、安定的で高品位の知識を提供し、それは、知識に基づく政策の形成や実施のための基礎を提供し、大勢の人々の生活の質を向上させ、そして、社会サービスの効率性を向上させうるものである。科学的な調査を促進するために、個人データは、EU 法又は加盟国の国内法に定める適切な要件及び保護措置の下、科学的研究の目的のために、取扱うことができる。

(158) Where personal data are processed for archiving purposes, this Regulation should also apply to that processing, bearing in mind that this Regulation should not apply to deceased persons. Public authorities or public or private bodies that hold records of public interest should be services which, pursuant to Union or Member State law, have a legal obligation to acquire, preserve, appraise, arrange, describe, communicate, promote, disseminate and provide access to records of enduring value for general public interest. Member States should also be authorised to provide for the further processing of personal data for archiving purposes, for example with a view to providing specific information related to the political behaviour under former totalitarian state regimes, genocide, crimes against humanity, in particular the Holocaust, or war crimes.
(158) 保管の目的のために個人データが取り扱われる場合、本規則は、死亡した者に対しては本規則が適用されないことに留意した上で、その取扱いにも適用されなければならない。公共の利益の記録を保有する公的機関又は公的組織若しくは民間組織は、EU 法又は加盟国の国内法により、一般的な公共の利益のための不朽の

価値を有する記録の収集、保存、鑑定、編纂、記述、送信、広報、普及及び配布をし、かつ、その記録へのアクセスを提供すべき法的義務をもつ公共機関でなければならない。加盟国は、例えば、かつての全体主義国家体制下の政治的活動、ジェノサイド、人道に対する罪、特に、ホロコースト、又は、戦争犯罪と関連する特別の情報を提供するという観点から、保管の目的のための個人データの追加的な取扱いを定めることも認められるものとしなければならない。

(159) Where personal data are processed for scientific research purposes, this Regulation should also apply to that processing. For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research. In addition, it should take into account the Union's objective under Article 179(1) TFEU of achieving a European Research Area. Scientific research purposes should also include studies conducted in the public interest in the area of public health. To meet the specificities of processing personal data for scientific research purposes, specific conditions should apply in particular as regards the publication or otherwise disclosure of personal data in the context of scientific research purposes. If the result of scientific research in particular in the health context gives reason for further measures in the interest of the data subject, the general rules of this Regulation should apply in view of those measures.
(159) 科学的研究の目的で個人データが取り扱われる場合、本規則は、その取扱いにも適用される。本規則の目的のために、科学的研究の目的のための個人データの取扱いは、例えば、技術開発及び展示、基礎研究、応用研究並びに民間資金の提供を受けた研究を含め、幅広く解釈されなければならない。加えて、欧州の研究領域を達成するという TFEU 第 179 条第 1 項に基づく EU の目的を考慮に入れなければならない。科学的研究の目的は、公衆衛生の領域において公共の利益において行われる研究も含めるものとしなければならない。科学的研究の目的のための個人データの取扱いの特殊性に適合させるため、特に、科学的研究の目的の過程における個人データの出版又はそれ以外の開示に関しては、特別の条件が適用されなければならない。特に、保険領域における科学的研究の結果が、データ主体の利益のため、追加的措置のための理由となる場合、そのような措置を考慮して、本規則の一般的な規定が適用されなければならない。

(160) Where personal data are processed for historical research purposes, this Regulation should also apply to that processing. This should also include historical research and research for genealogical purposes, bearing in mind that this Regulation should not apply to deceased persons.
(160) 歴史的研究の目的で個人データが取り扱われる場合、本規則は、その取扱いにも適用される。これは、歴史的研究及び地理調査の目的も含むが、死亡した者に対しては本規則が適用されないことに留意する。

(161) For the purpose of consenting to the participation in scientific research activities in clinical trials, the relevant provisions of Regulation (EU) No 536/2014 of the European Parliament and of the Council [15] should apply.
(161) 臨床試験における科学的な研究活動への参加に同意する目的のためには、欧州議会及び理事会の規則 (EU) No 536/2014[15]の関連条項が適用されなければならない。

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

[15] Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC (OJ L 158, 27.5.2014, p. 1).
人間用の医療機器の臨床試験に関する、及び、指令 2001/20/EC を廃止する欧州議会及び理事会の 2014 年 4 月 16 日の規則 (EU) No 536/2014（OJ L 158, 27.5.2014, p.1）

not used in support of measures or decisions regarding any particular natural person.
(162) 統計の目的のために個人データが取扱われる場合、本規則は、その取扱いに適用される。EU 法又は加盟国の国内法は、本規則の制限の範囲内で、統計の内容、アクセス管理、統計の目的による個人データの取扱いの仕様、並びに、データ主体の権利及び自由の安全性を確保し、統計上の秘密を確保するための適切な措置を定めなければならない。統計の目的とは、統計調査又は統計結果の作成のために必要となる個人データの収集及び取扱いの業務遂行のことを意味する。統計結果は、科学的研究の目的を含め、さらに、異なる目的のために用いることができる。統計の目的とは、統計の目的による取扱いの結果が、個人データではなく、集約されたデータであること、そして、その結果又は個人データが特定の自然人に関する措置又は決定を支援する際に用いられるものではないことを意味する。

(163) The confidential information which the Union and national statistical authorities collect for the production of official European and official national statistics should be protected. European statistics should be developed, produced and disseminated in accordance with the statistical principles as set out in Article 338(2) TFEU, while national statistics should also comply with Member State law. Regulation (EC) No 223/2009 of the European Parliament and of the Council [16] provides further specifications on statistical confidentiality for European statistics.
(163) EU の公式統計及び加盟国の公式統計を作成するために EU の統計局及び加盟国の統計局が収集する機密性のある情報は、保護されなければならない。欧州統計は、TFEU の第 338 条第 2 項に定める統計上の基本原則に従って設けられ、作成され、かつ、配布されるものとしなければならない。他方において、加盟国の統計は、加盟国の国内法を遵守しなければならない。欧州議会及び理事会の規則(EC) No 223/2009[16]は、欧州統計のために統計上の秘密に関する別の細則を定めている。

(164) As regards the powers of the supervisory authorities to obtain from the controller or processor access to personal data and access to their premises, Member States may adopt by law, within the limits of this Regulation, specific rules in order to safeguard the professional or other equivalent secrecy obligations, in so far as necessary to reconcile the right to the protection of personal data with an obligation of professional secrecy. This is without prejudice to existing Member State obligations to adopt rules on professional secrecy where required by Union law.
(164) 管理者又は処理者から個人データへのアクセス及びその施設へのアクセスを得るための監督機関の権限に関し、加盟国は、法律により、本規則の制限の範囲内で、個人データの保護の権利と職務上の守秘義務との整合性を保つために必要となる範囲内において、職務上の秘密又はそれと均等の機密保持義務を保護するための特別規定を採択できる。これは、EU 法によって要求される場合、職務上の守秘義務に関する法令を採択すべき加盟国の既存の義務を妨げるものではない。

(165) This Regulation respects and does not prejudice the status under existing constitutional law of churches and religious associations or communities in the Member States, as recognised in Article 17 TFEU.
(165) 本規則は、TFEU の第 17 条において承認されているように、加盟国内にある教会、宗教団体及び宗教上の集団の現行の憲法に基づく地位を尊重し、かつ、これを妨げない。

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

[16] Regulation (EC) No 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No 1101/2008 of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) No 322/97 on Community Statistics, and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities (OJ L 87, 31.3.2009, p. 164).
欧州の統計に関する、並びに、欧州共同体統計局に対する統計上の秘密に服するデータの移転に関する欧州議会及び理事会の規則(EC, Euratom) No 1101/2008 を廃止し、欧州共同体の統計に関する理事会規則(EC) No 332/97 を廃止し、及び、Euratom の欧州委員会統計計画委員会の設置に関する理事会決定 89/382/EEC を廃止する欧州議会及び理事会の 2009 年 5 月 11 日の規則(EC) No 223/2009（OJ L 87, 31.3.2009, p.164）

the Union, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission. In particular, delegated acts should be adopted in respect of criteria and requirements for certification mechanisms, information to be presented by standardised icons and procedures for providing such icons. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level. The Commission, when preparing and drawing-up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and to the Council.
(166) 本規則の目的、すなわち、自然人の基本的な権利及び自由、特に、自然人の個人データ保護の権利を保護し、かつ、EU 域内における個人データの自由な移転を確保するために、TFEU の第 290 条による行為を採択する権限が欧州委員会に委任される。特に、認証方法の基準及び要件、標準化されたアイコンによって表示されるべき情報及びそのアイコンを提供する手続に関して、委任される行為が採択されなければならない。専門家レベルのものを含め、欧州委員会がその作業を準備する間に適切に協議を行うことは、特に重要なことである。欧州委員会は、委任された行為を準備し、起草する際、欧州議会及び理事会に対し、同時に、適時に、かつ、適切に、関連文書を送付することを確保しなければならない。

(167) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission when provided for by this Regulation. Those powers should be exercised in accordance with Regulation (EU) No 182/2011. In that context, the Commission should consider specific measures for micro, small and medium-sized enterprises.
(167) 本規則の実装のための統一的な条件を確保するため、本規則によって定められている場合、欧州委員会に対してその実装権限が与えられなければならない。この権限は、規則(EU) No 182/2011 に従って行使されなければならない。その過程において、欧州委員会は、中小零細企業のための具体的な措置を検討しなければならない。

(168) The examination procedure should be used for the adoption of implementing acts on standard contractual clauses between controllers and processors and between processors; codes of conduct; technical standards and mechanisms for certification; the adequate level of protection afforded by a third country, a territory or a specified sector within that third country, or an international organisation; standard protection clauses; formats and procedures for the exchange of information by electronic means between controllers, processors and supervisory authorities for binding corporate rules; mutual assistance; and arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board.
(168) 管理者と処理者の間及び処理者間における標準約款；行動準則；認証のための技術基準及び認証方法；第三国、第三国内における地域若しくは特定の部門又は国際機関によって与えられる十分なレベルの保護；標準データ保護約款；拘束的企業準則のための管理者、処理者及び監督機関間の電子的な手段による情報交換のフォーマット及び手続；共助；監督機関の間及び監督機関と委員会の間での電子的な手段による情報交換のための手配に関する実装行為の採択のために、審議手続が用いられなければならない。

(169) The Commission should adopt immediately applicable implementing acts where available evidence reveals that a third country, a territory or a specified sector within that third country, or an international organisation does not ensure an adequate level of protection, and imperative grounds of urgency so require.
(169) 利用可能な証拠によって、第三国、第三国内の地域若しくは特定の部門又は国際機関が十分なレベルの保護を確保していないことが明らかになり、かつ、緊急性という正当化根拠があるときは、欧州委員会は、直ちに、適用可能な実装行為を採択しなければならない。

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

proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.
(170) 本規則の目的、すなわち、EU 全域における自然人の保護及び個人データの自由な移転の均等なレベルでの確保は、加盟国によっては十分に達成することができず、そのような行為の規模及び効果のゆえに、EU レベルでより良くその目的を達成することができるものであるから、EU は、欧州連合条約（TFU）の第 5 条に定める補完性原則に従い、措置を採択できる。同条に定める比例性原則に従い、本規則は、その目的を達成するために必要なところを超えることがない。

(171) Directive 95/46/EC should be repealed by this Regulation. Processing already under way on the date of application of this Regulation should be brought into conformity with this Regulation within the period of two years after which this Regulation enters into force. Where processing is based on consent pursuant to Directive 95/46/EC, it is not necessary for the data subject to give his or her consent again if the manner in which the consent has been given is in line with the conditions of this Regulation, so as to allow the controller to continue such processing after the date of application of this Regulation. Commission decisions adopted and authorisations by supervisory authorities based on Directive 95/46/EC remain in force until amended, replaced or repealed.
(171) 指令 95/46/EC は、本規則によって廃止される。本規則が適用される日において既に行われている取扱いは、本規則の発効の後 2 年以内に、本規則に適合するようにされなければならない。取扱いが指令 95/46/EC による同意に基づくものである場合、その同意を与えた態様が本規則の条件に沿うものである限り、本規則の適用の日の後に管理者がその取扱いを継続することができるようにするために、データ主体が自己の同意を重ねて提供することを要しない。指令 95/46/EC に基づいて採択され、監督機関によって承認された欧州委員会の決定は、その改正、置き換え又は廃止があるまでの間は、その有効性を維持する。

(172) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on 7 March 2012 [17].
(172) 欧州データ保護監察機関は、規則(EC) No 45/2001 の第 28 条第 2 項に従って協議をし、2012 年 3 月 7 日にその意見書を[17]提出した。

(173) This Regulation should apply to all matters concerning the protection of fundamental rights and freedoms vis-à-vis the processing of personal data which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC of the European Parliament and of the Council [18], including the obligations on the controller and the rights of natural persons. In order to clarify the relationship between this Regulation and Directive 2002/58/EC, that Directive should be amended accordingly. Once this Regulation is adopted, Directive 2002/58/EC should be reviewed in particular in order to ensure consistency with this Regulation,
(173) 本規則は、管理者の義務及び自然人の権利を含め、欧州議会及び理事会の指令 2002/58/EC[18]に定めるのと同じ特別の義務に服さない個人データの取扱いとそれぞれ対応する基本的な権利及び自由の保護に関する全ての事柄に適用される。本規則と指令 2002/58/EC との関係を明確にするため、同指令は、しかるべく改正されなければならない。本規則が採択された後、指令 2002/58/EC は、特に本規則との整合性を確保するために、見直されなければならない。

HAVE ADOPTED THIS REGULATION:

---

[17] OJ C 192, 30.6.2012, p. 7.
OJ C 192, 30.6.2012, p. 7.
[18] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).
電子通信分野における個人データの保護及びプライバシーの保護に関する欧州議会及び理事会の 2002 年 7 月 12 日の指令 2002/58/EC（プライバシー及び電子通信に関する指令）（OJ L 201, 31.7.2002, p.37）