REGULATION (EU) 2016/… OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL	개인정보의 처리와 관련한 개인의 보호 및 개인정보의 자유로운 이동에 관한 유럽의회와 유럽이사회 규정 (EU) No XXX/20161)
# 원문	# 해설전문 번역
(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) 개인정보처리의 보호는 개인의 기본적인 권리이다. 유럽연합 기본권 헌장(이하 '헌장') 제8조 (1)항과 유럽연합기능조약(이하 TFEU)의 제 16조 (1)항에서는 모든 사람은 본인의 개인정보를 보호할 권리가 있다고 규정하고 있다.
(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) 자연인의 개인정보처리 보호, 특히 개인정보 보호는 개개인의 국적 또는 거주지에 상관없이 개인의 기본적 권리와 자유로써 존중되어져야 함을 기본원칙으로 한다. 이 법은 자유, 안보 및 정의와 경제연합 분야의 성과, 경제 및 사회적 발전, 역내 시장 경제의 강화 및 통합, 그리고 개인의 복지 증진을 목적으로 한다.
(3) Directive 95/46/EC of the European Parliament and of the Council[1] seeks to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to ensure the free flow of personal data between Member States. [1] 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).	(3) 유럽의회 및 유럽각료이사회의 지침 95/46/EC는 개인정보처리 활동에 있어 개인의 기본적 권리와 자유가 통일적으로 보호될 수 있도록 하며, 회원국 간에는 개인정보가 자유롭게 이동될 수 있도록 한다.
(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) 개인정보처리는 인류에 기여할 수 있도록 설계되어야 한다. 개인정보보호권은 절대적 권리가 아니며, 개인정보보호권은 사회에서의 개인정보보호 기능과 관련하여 고려되어야 하며 비례의 원칙에 입각하여 다른 기본권과 균형을 이루어야 한다. 이 법은 모든 기본권을 존중하고, 여러 협약에서 구현되고 있는 헌장(Charter)의 자유와 원칙을 준수한다. 이러한 협약에는 특히 사생활 및 가족생활, 가정과 통신을 존중할 권리, 개인정보보호, 사상과 양심 및 종교의 자유, 표현 및 정보의 자유, 기업 활동의 자유, 효과적인 구제 권리와 공정한 재판을 받을 권리, 그리고 문화적, 종교적, 언어적 다양성 등이 포함된다.

(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) 역내시장에서 경제적·사회적으로 기능이 통합됨에 따라 회원국 간 개인정보 교류가 크게 증가했다. 유럽 연합 내에서의 개인, 협회와 사업체 등, 공공 및 민간 주체 사이의 개인정보 교류가 증가해왔다. 회원국의 기관들은 유럽연합 법률에 따라 기관의 업무를 수행하기 위한 목적이나, 또 다른 회원국의 기관을 대신하여 업무를 수행하기 위한 목적으로 협력하고 개인정보를 교류해야 할 것을 요청받고 있다.
(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) 격한 기술발전과 세계화에 따라 개인정보보호 분야에 새로운 도전이 제기되었다. 개인정보의 수집 및 공유 규모가 상당한 수준으로 확대되었다. 기술을 통해 민간기업과 공공기관이 업무수행을 위해 전례 없는 규모로 개인정보를 활용하게 되었다. 개인은 개인정보를 공적으로 세계적으로 활용할 수 있다. 기술은 경제와 사회생활을 변화시켜왔다. 앞으로는 기술을 통해 유럽 역내의 자유로운 정보 이동과 제 3국 및 국제기구로의 개인정보 이전을 용이하게 하고, 개인정보를 높은 수준으로 보호해야 한다.
(7) Those developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market. Natural persons should have control of their own personal data. Legal and practical certainty for natural persons, economic operators and public authorities should be enhanced.	(7) 역내시장에서 디지털 경제를 발전시키기 위해서 신뢰 구축이 중요하다는 점을 고려하면, 강력한 집행력을 기반으로 하는 유럽연합에 더 강력하고 일관성 있는 개인정보보호 프레임워크(framework)가 필요하다. 개인은 본인의 개인정보에 대한 통제권을 보유해야 한다. 개인, 경제주체 및 공공기관을 위한 법적, 실질적 확실성이 강화되어야 한다.
(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) 이 법의 세부규정 및 제한사항을 각 회원국의 법률로써 규정하는 경우에는, 회원국은 일관성을 유지하고 회원국 법률의 수범자가 국가법률 규정을 이해하는 데 필요할 경우 자국법에 편입할 수 있다.
(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) 지침 95/46/EC에 명시된 목적과 원칙은 여전히 타당하지만, 해당 지침은 유럽 내에서 개인정보보호 방침을 집행하는 데 일관성이 결여되는 문제가 있었거나, 법적으로 확실하지 않았거나, 또는 온라인으로 활동하는 개인을 보호하는데는 상당한 리스크가 있다. 광범위하고도 일반적인 인식을 막지는 못하였다. 국가마다 개인정보보호권 등 개인의 권리와 자유의 보호 수준이 차이남으로 인하여 유럽 전체의 자유로운 개인정보의 흐름을 방해할 수 있다. 이러한 차이는 유럽연합 차원의 경제활동을 추구하는 데 장애물이 되거나, 경쟁을 왜곡하고 유럽연합 법률에 따른 기관들이 맡은 임무를 수행하는 데 방해할 수 있다. 각 국의 보호 수준이 상이한 이유는 지침 95/46/EC의 집행 및 적용상의 차이가 있었기 때문이다.

(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) 일관성을 유지하고 개인을 높은 수준으로 보호하며 역내 개인정보의 이동을 막는 장애물을 제거하기 위해서, 각 국은 개인정보처리에 있어, 개인의 권리와 자유를 동일한 수준으로 보호해야한다. 개인정보처리에 관련된 개인의 기본권과 자유를 보호하기 위한 규정은 유럽 전역에 일관적이고 동일하게 적용되어야 한다. 공익을 위한 업무를 수행하거나 처리자에게 위임된 공적 권한을 집행하기 위하여 개인정보를 처리하는 경우에 대해, 회원국은 추가적으로 이 법 규정을 적용한다는 국내법 조문을 (있었다면) 그대로 유지하거나, (없었다면) 새로이 만들어야 한다. 회원국은, 전 분야를 아우르는 일반법인 개인정보 이행지침 95/46/EC와 연계하여, 특별 규정이 필요한 분야에 있어서는 분야별 규정을 둔다. 또한 이 법은 회원국이 특정범주의 개인정보('민감정보')처리 등에 관한 국가법을 명시할 수 있도록 회원국 재량을 보장한다. 이런 점에서, 이 법은 개인정보처리가 적법하다고 판단되는 상황에 대한 결정 등, 특정한 정보처리 환경을 규정하는 회원국의 법률을 배제하지 않는다.
(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) 유럽연합 전역에서 개인정보를 보호하는 데 있어 정보주체의 권리와 개인정보를 처리하거나 처리를 결정하는 사람들의 의무를 상세하게 규정하는 것이 효과적으로 개인정보를 보호하는 데 필수적이다. 또한 개인정보보호에 대한 규정을 준수하고 감시(monitoring)할 수 있는 동일한 권한과 회원국의 개인정보 침해에 대해 제재할 수 있는 동일한 벌칙권한도 필수적이다.
(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) TFEU의 제 16조 (2)항은 유럽의회와 각료이사회가 개인정보처리에 관련된 개인을 보호하는 규정과 개인정보의 자유로운 이동에 관한 규정을 정하도록 명하고 있다.
(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	(13) 유럽연합 내에서 개인의 보호수준을 일관적으로 보장하고 이 법은 역내시장에서 서로의 차이로 인하여 자유로운 개인정보 이동이 방해받지 않도록 영세, 중소기업을 포함한 경제인을 위해 법적 확실성과 투명성을 제공하고, 회원국의 개인에게 법적으로 집행 가능한 권리와 정보처리자 및 수탁처리자의 의무와 책임을 동일한 수준으로 제공하며, 개인정보처리에 대한 일관적인 감시와 회원국 내 동일한 제재권한과 다른 회원국 간 감독기구 사이의 효과적인 협력을 보장하기 위해서 필요하다. 역내시장이 적절하게 기능을 발휘하기 위하여는 개인정보처리 관련 개인보호와 연계되었다는 이유로 유럽연합 내 개인정보의 자유로운 이동을 제재하거나 금지하지 않아야 한다. 영세 및 중소기업의 특정 상황을 고려하기 위해, 이 법은 기록작성과 관련된 250명 미만의 기관에 대해서는 그 적용을 일부 제외시키는 조문을 포함한다. 또한 유럽연합 기관이나 기구가 이 법을 적용할 때는 중소기업의 구체적인 니즈

requires that the free movement of personal data within the Union is not restricted or prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data. To take account of the specific situation of micro, small and medium-sized enterprises, this Regulation includes a derogation for organisations with fewer than 250 employees with regard to record-keeping. In addition, the Union institutions and bodies, and Member States and their supervisory authorities, are encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation. The notion of micro, small and medium-sized enterprises should draw from Article 2 of the Annex to Commission Recommendation 2003/361/EC[1].

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

(needs)를 고려하도록 지향하여야 한다. 중소기업의 개념은 위원회 권고 2003/361/EC에 대한 부록 제2조에 따라야 한다.

(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) 이 법에서 정하는 개인정보보호는 국적이나 거주지에 상관없이 개인정보처리와 관련된 개인에게 적용되어야 한다. 이 법은 법인과 법인으로 설립된 사업체의 개인정보인 이름, 법인의 형태, 법인의 연락처 등에 대한 처리는 포함되지 않는다.

(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) 기술적 문제(circumvention)로 인한 심각한 위험을 방지하기 위해서, 개인보호는 기술적으로 중립적이어야하며, 사용되고 있는 기술에 의존해서는 안된다. 개인정보가 파일링시스템에 보관되어 있거나 보관될 예정이라면, 자동화 또는 개인정보처리를 할 경우 개인에 대한 보호책도 적용되어야 한다. 구체적 기준에 따라 정렬되지 않은 개인정보에 대한 커버 페이지와 파일, 그리고 파일세트는 이 법의 적용범위에 해당하지 않는다.

(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) 이 법은 기본권 및 자유보장에 관한 사안과 국가안보 활동과 같이 유럽연합 법률의 범위 외의 활동에 따라 자유롭게 이동하게 되는 개인정보에는 적용되지 않는다. 이 법은 회원국이 유럽연합 내 일반외교 및 안보정책과 관련한 업무를 수행할 때 시행하는 개인정보처리에는 적용되지 않는다.

(17) Regulation (EC) No 45/2001 of the European Parliament and of the Council[1] applies to the processing of personal data by the Union institutions, bodies, offices and agencies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data should be adapted to the principles and rules established in 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

(17) 유럽의회와 유럽각료이사회의 규정(EC) No 45/2001은 유럽연합의 기관 및 기구가 처리하는 개인정보에 적용된다. 이러한 개인정보처리에 적용 가능한 규정(EC) No 45/2001 및 기타 유럽연합 법률은 이 법의 원칙과 규정에 맞게 조정되어야하며 이 법에 따라 적용되어야 한다. 유럽연합에서 더 강력하고 일관된 개인정보보호 프레임워크를 제공하기 위해서는 이 법을 채택한 후, 이 법과 동시에 적용시키기 위해 규정(EC) No 45/2001을 필요한 만큼 개정하여야 한다.

application at the same time as this Regulation.

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

(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) 이 법은 순수한 개인활동 또는 가정활동 과정으로, 업무 활동이나 상업 활동과 연관이 없는 활동의 과정에서 개인이 수행하는 개인정보의 처리에는 적용되지 않는다. 개인활동이나 가정활동에는 서신, 주소지 보유이나 소셜네트워킹 그리고 이러한 활동에서 이루어진 온라인 활동 등이 포함될 수 있다. 그러나 이러한 개인 활동이나 가정활동을 위해 개인정보를 처리하기 위한 수단을 제공하는 정보처리자나 수탁처리자에게는 이 법이 적용된다.

(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/… of the European Parliament and of the Council[1] [2]. Member States may entrust competent authorities within the meaning of Directive (EU) 2016/… [3] 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.

(19) 범죄예방, 조사, 적발 또는 기소, 형사처벌의 목적이나 공공안보에 대한 위협으로부터 보호·예방, 개인정보의 자유로운 이전 등을 목적으로 관련 기관이 개인정보를 처리할 때는 유럽연합의 특별법대로 개인정보가 보호되므로 이 법은 적용되지 않는다. 공공안보에 대한 위협으로의 보호·예방, 개인정보의 자유로운 이전, 범죄 예방, 조사, 적발 또는 기소, 형사처벌을 위해 필수적인 업무가 아닌 업무를 위임할 수 있고 이러한 업무(공공안보 등에 필수적이지 않은 업무)와 관련된 개인정보처리는 유럽연합 법률의 적용범위에 해당하는 한 이 법의 범위에 해당한다. 이 법 적용범위의 목적으로 관할기관이 개인정보를 처리하는 것과 관련하여, 회원국은 이 법의 적용과 맞추기 위하여 더 구체적인 규정(provisions)을 유지하거나 새로이 둘 수 있어야 한다. 이와 같은 규정을 통해 각 회원국이 헌법적, 조직적, 행정적 구조를 참작하여 관할기관이 기타업무(공공안보 등에 필수적이지 않은 업무)를 처리할 때 개인정보 처리에 대한 구체적 요건들이 더 정확히 결정될 수 있다. 민간기관의 개인정보처리가 이 법의 범위에 해당할 때, 이 법은 회원국이 특정조건에 따라 특정한 의무 및 권리를 제한할 수 있음을 규정해야 한다. 단, 그 같은 제한이 공공안보에 대한 위협으로의 보호·예방, 개인정보의 자유로운 이전, 범죄 예방, 조사, 적발 또는 기소, 형사처벌의 집행 등 민주사회에서 필요하고 적절한 조치가 될 때 그러하다. 예를 들어, 돈세탁 방지 프레임워크나 법의학연구 활동이 이에 해당한다.

[1] Directive (EU) 2016/… of the European Parliament and of the Council 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 (OJ L …).

[2] OJ: Please insert the number of the Directive in doc. st 5418/16 and the publication reference.

[3] OJ: Please insert the number of the Directive in doc. st 5418/16.

With regard to the processing of personal data by those competent authorities for purposes falling within scope of this Regulation, Member States should be able to maintain or introduce more specific provisions to adapt the application of

the rules of this Regulation. Such provisions may determine more precisely specific requirements for the processing of personal data by those competent authorities for those other purposes, taking into account the constitutional, organisational and administrative structure of the respective Member State. When the processing of personal data by private bodies falls within the scope of this Regulation, this Regulation should provide for the possibility for Member States under specific conditions to restrict by law certain obligations and rights when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific important interests including public security and the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. This is relevant for instance in the framework of anti-money laundering or the activities of forensic laboratories.	
(20) While this Regulation applies, inter alia, to the activities of courts and other judicial authorities, Union or Member State law could specify the processing operations and processing procedures in relation to the processing of personal data by courts and other judicial authorities. The competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of the judiciary in the performance of its judicial tasks, including decision-making. It should be possible to entrust supervision of such data processing operations to specific bodies within the judicial system of the Member State, which should, in particular ensure compliance with the rules of this Regulation, enhance awareness among members of the judiciary of their obligations under this Regulation and handle complaints in relation to such data processing operations.	(20) 이 법은 특히 법원과 기타 사법기관의 활동에 적용되며, 유럽연합법률이나 회원국 법률은 법원과 기타 사법기관이 수행하는 개인정보처리와 관련한 처리절차 및 처리 방식을 규정할 수 있다. 법원이 사법권한을 행사하기 위하여 개인정보를 처리할 때는 감독기관이 그 권한을 행사하면 아니된다. 이는 사법활동의 수행, 의사결정 등 사법부의 독립성을 보장하기 위함이다. 회원국의 사법권 체계에 소속된 특정 기관들은 관련 개인정보처리 과정에 대해 감독권을 위임받을 수 있다. 이러한 기관들은 이 법의 규정을 준수해야 하고 이 법에 따른 법조인의 의무에 대한 인식을 높여야하며, 개인정보처리 과정에 관한 민원을 처리해야 한다.
(21) This Regulation is without prejudice to the application of Directive 2000/31/EC of the European Parliament and of the Council[1], 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. [1] 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).	(21) 이 법은 유럽의회 및 유럽각료이사회의 지침 2000/31/EC 중 특히, 제12조에서 제 15조까지 규정되어있는, 중개서비스 제공자(intermediary service providers)에 대한 손해배상 원칙(liability rules)의 적용을 침해하지 않는다. 중개서비스 제공자에 대한 손해배상 원칙이 그대로 적용된다. 해당 지침은 회원국 간 정보사회서비스의 자유로운 이동을 보장하여 역내 시장이 적절하게 기능할 수 있도록 기여 한다.
(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.	(22) 유럽 내 정보처리자 또는 수탁처리자가 사업장(establishment)의 활동과 관련하여 행하는 개인정보 처리는 이 법에 따라 진행되어야 하며, 실제 처리가 유럽 내에서 발생하는 지 여부와는 상관없다. 사업장이라 함은 안정적인 방식을 통해 효과적으로 실제 활동을 수행하는 것을 의미한다. 이러한 사업장 설립 형태는, 법인격을 지닌 분점이든 자회사든 상관없다.

(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) 개인이 이 법에서 정하는 바 대로 보호받을 수 있도록 하기 위해서, 유럽 연합 역내에 있는 정보주체에 대한 개인정보를 유럽연합 역외지역에 설립된 정보처리자 또는 수탁처리자가 처리하는 경우에도 이 법의 적용을 받아야 하며, 유럽연합 역내 정보주체에게 재화나 서비스를 제공하는 것과 관련한 처리활동인 경우 이에 대한 실제로 비용 지불과 관련이 있는 지의 여부와 상관이 없이 이 법이 적용된다. 유럽 연합 역외의 정보처리자가 수탁처리자가 역내의 정보주체에게 재화나 서비스를 제공했는 지 여부를 결정하기 위해서는 해당 정보처리자나 수탁처리자가 유럽연합 역내의 하나 또는 그 이상의 회원국의 정보주체에게 서비스를 제공하는 것이 예상될 수 있었는 지의 여부가 명백해야 한다. 정보처리자가 단지 유럽연합 역내에서 정보처리자, 수탁처리자 또는 중개인의 웹사이트에 접근할 수 있다거나 이메일 주소 또는 기타 연락처를 열람할 수 있다는 것으로는 이와 같은 확실한 의사가 있었다고 보기는 불충분하며, 하나 이상의 회원국에서 통용되는 언어나 통화를 사용하고 그 언어로 재화와 서비스를 주문할 가능성이 있다거나, 유럽연합 역내의 소비자나 이용자에 대해 언급한 적이 있는 경우에는, 정보처리자가 유럽연합 내의 정보주체에게 재화나 서비스를 제공하고자 하는 확실한 의사가 있었다고 판단될 수 있다.
(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) 역내 지역에 설치하지 않은(역외에 설치한) 정보처리자 또는 수탁처리자가, 유럽 연합 역내에 있는 정보주체의 개인정보를 처리하는 경우는, 해당 정보처리자 또는 수탁처리자가 역내에서 이루어지는 정보주체의 행동을 감시(monitoring)하는 것과 관련있을 때 이 법을 적용받는다. 이러한 정보처리가 정보주체의 활동을 감시(monitor)하는 것이라고 할 만한 것인지를 결정하기 위해서는, 개인이 인터넷 상에서 추적되는 여부가 명백해야 하는데, 특히 정보주체에 대한 결정을 할 때나, 정보주체의 개인적 선호, 행동과 태도를 분석하거나 예상하는 등의 프로파일링 기법 같은 개인정보처리 기술을 잠재적·계속적으로 사용하는 것과 같은 방법으로 추적되는 것을 말한다.
(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) 회원국 법률이 국제법의 효력으로 적용되는 경우, 이 법은 회원국 내의 설립된 외교공관이나 영사관 등 유럽연합 역외 지역에 설립된 정보처리자에게도 적용될 수 있다.
(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	(26) 개인정보보호원칙은 식별되었거나 또는 식별될 수 있는 개인에 관한 일체의 정보에 적용될 수 있다. 가명처리 정보는, 추가 정보를 이용하여 개인을 식별할 수 있는 정보로서 식별할 수 있는 개인정보로 간주되어야 한다. 어떤 개인이 식별 가능한지를 판단하기 위해서는 특정개인의 식별 등 처리자 또는 제3자 모두가 개인을 직접 또는 간접적으로 확인하기 위해 사용할 것으로 합리적으로 예상되는(reasonably likely) 모든 수단을 고려해야 한다. 개인을 식별하기 위해 사용될 것으로 합리적으로 예상되는 수단인지를 확인하기 위해서는, 식별하기 위해 소요되는 비용과 시간 등 객관적인 요소를 모두 고려하고, 처리 당시 가용한 기술과 기술적 발전을 모두 고려하여야 한다. 익명정보에는 개인정보보호원칙이 적용되지 않는다. 다시 말해서 이 원칙은 식별

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.	되었거나 또는 식별될 수 있는 개인과 관련되지 않는 정보 또는 그런 방식으로 익명처리되어 더 이상 식별될 수 없는 정보주체에는 적용되지 않는다. 따라서 이 법은 통계목적 및 연구 목적 등을 위한 익명정보의 처리에는 적용되지 않는다.
(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) 이 법은 망자의 개인정보에 적용되지 않는다. 회원국은 망자의 개인정보 처리에 대한 규정을 제공할 수 있다.
(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) 개인정보에 가명처리를 적용하는 것은 관련 정보주체에게 미치는 위험성을 줄이고 컨트롤러와 프로세서가 개인정보 보호의 의무를 충족시킬 수 있도록 지원한다. 본 규정에서 명시적으로 '가명처리'를 도입하는 것이 기타의 개인정보 보호의 조치를 배제시키려는 의도는 아니다(가명처리를 하더라도 기타의 개인정보 보호 조치를 적용할 필요도 있음).
(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) 개인정보의 처리 시 가명처리 적용에 대한 인센티브를 부여하기 위해서는 가명처리 조치가 일반적 분석은 허용하되 동종의 컨트롤러 사업체 내에서 가능할 수 있어야 한다. 이 때 동종의 컨트롤러 사업체 내의 컨트롤러는 관련 처리에 대하여 본 규정이 이행되고 개인정보를 특정 정보주체에 연결시키는 추가 정보를 별도 보관하도록 하는 기술적·관리적 조치를 취했어야 한다. 개인정보를 처리하는 컨트롤러는 동종의 컨트롤러 사업체 내의 인가받은 사람을 가리킨다.
(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.	(29) 개인정보의 처리 시 가명처리 적용에 대한 인센티브를 부여하기 위해서는 가명처리 조치가 일반적 분석은 허용하되 동종의 컨트롤러 사업체 내에서 가능할 수 있어야 한다. 이 때 동종의 컨트롤러 사업체 내의 컨트롤러는 관련 처리에 대하여 본 규정이 이행되고 개인정보를 특정 정보주체에 연결시키는 추가 정보를 별도 보관하도록 하는 기술적·관리적 조치를 취했어야 한다. 개인정보를 처리하는 컨트롤러는 동종의 컨트롤러 사업체 내의 인가받은 사람을 가리킨다.
(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	(31) 관세청과 국세청, 금융조사기관, 독립행정기관, 또는 증권시장 규제 및 감독 책임의 금융시장 기구 등, 공적 임무 수행을 위해 법적 의무에 따라 개인정보를 제공받는 공공기관은 유럽연합법률 또는 회원국 법률에 따라 일반적 이익에 관한 특정 조회업무를 수행하기 위해 필요한 개인정보를 받은 경우, 공공기관은 정보수령인으로 간주되지 않는다. 공공기관은 반드시 서면으로 개인정보 제공을 요청해야 한다. 이는 합리적인 이유가 있어야하고 간헐적이어야 하며, 파일링 시스템 전체에 대한 요청이 아니어야한다. 파일링시스템끼리 연결되는 결과를 초래하지 않아야 한다. 개인정보를 처리할 때 처리의 목적에 관한 적용가능한 개인정보보호 규정이 준수되어야 한다.

writing, reasoned and occasional and should not concern the entirety of a filing system or lead to the interconnection of filing systems. The processing of personal data by those public authorities should comply with the applicable data-protection rules according to the purposes of the processing.	
(32) Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.	(32) 동의는 전자적 방법을 포함한 서면진술이나 구두진술 등으로, 정보주체가 개인정보의 처리에 대해 자유롭게 제공하여야 하는데, 구체적으로, 고지된 명확한 합의를 나타내주는 적극적인 행위로써 제공되어야 한다. 동의표현방법에는 인터넷 웹사이트의 개인정보처리동의란 체크, 정보사회서비스에 대한 기술적 설정 선택 또는 본인의 개인정보처리 수락을 의미하는 정보주체의 행동이나 기타 진술이 포함된다. 따라서 침묵, 사전 자동체크 된 개인정보처리동의나 부작위는 동의에 해당되지 않는다. 동의는 단일 또는 복수의 동일한 목적을 위한 모든 처리 활동에 유효하다. 복수의 목적으로 개인정보를 처리하는 경우, 각 목적에 대한 동의를 받아야 한다. 만약 정보주체의 동의를 전자방식의 요청에 따라 제공하는 경우, 그 요청은 명확하고 간결하게 제공되어야 하며, 관련 서비스 이용을 불필요하게 방해해서는 안된다.
(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) 과학적 연구목적의 경우, 개인정보 수집 당시에 개인정보 처리목적을 충분히 확인하기가 불가능할 때가 많다. 따라서 정보주체는 과학적 연구의 공인된 윤리 기준에 부합된 경우, 특정 연구 분야에 한해 동의를 제공할 수 있다. 정보주체는 의도한 처리목적이 허용하는 선에서 특정 연구 분야 혹은 연구 일부분에 한해 본인의 동의를 제공할 수 있어야 한다.
(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) 유전자정보는 개인의 유전적 또는 후천적으로 얻은 유전자 특성에 관한 개인정보로 정의되어야 하며 이 유전자 특성은 염색체 분석, 데옥시리보핵산(DNA) 분석 또는 리보핵산(RNA)분석 등 해당 개인으로부터 채취한 생물학적 샘플 분석에서 얻은 결과 또는 다른 요소 분석을 통해 이에 상응하는 정보를 획득하여 얻은 결과이다.
(35) Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council[1] to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination	(35) 건강관련 개인정보에는 정보주체의 과거, 현재, 혹은 미래의 신체적 또는 정신적 건강 상태의 정보를 드러내는 모든 정보주체의 건강상태에 속하는 정보가 포함된다. 이 정보에는 유럽의회와 각료이사회의 지침 2011/24/EU에 규정된 바와 같이 의료보호서비스를 등록하고 정보주체에 제공하는 과정에서 수집된 개인에 대한 정보도 포함된다. 건강목적으로 특정 개인을 식별하기 위해 개인에게 부여되는 숫자, 상징, 혹은 특별사항도 포함되며, 유전자 정보와 생물학적 샘플 등, 신체의 일부분 또는 신체 물질에 대한 테스트나 검사에서 얻은 정보도 포함된다. 또한 질병, 장애, 질병 위험성, 의료 내역, 임상치료에 대한 정보 또는, 이와 무관하게, 내과의사 혹은 다른 의료계 종사자, 병원, 의료기기나 시험관 진단검사에서 얻은 정보주체에 대한 생리학적 상태 혹

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.

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

은 생체의학적 상태에 대한 정보도 포함된다.

(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 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) 정보처리자의 유럽연합 역내 주 사업장(establishment)은 정보처리자의 유럽연합 내 중앙행정 지점이어야 하지만, 개인정보 처리 수단과 목적에 대한 결정을 유럽연합 내 다른 사업장(establishment)에서 정하는 경우, 그 다른 사업장이 주 사업장으로 간주되어야 한다. 정보처리자의 유럽 내 주 사업장은 객관적인 기준 따라 결정되어야하며, 안정적인 방식을 통해 관리활동을 효과적·실제적으로 수행하는 것을 의미하는데, 관리활동이란 처리목적 및 수단에 대해 주요 결정을 내리는 것을 말한다. 이 기준은 개인정보처리 활동이 해당 지역에서 수행되는지 여부에 따라 결정되어서는 안된다. 개인정보처리 또는 처리활동을 위한 기술적 수단과 기술이 존재하거나 이러한 기술 등을 활용하는 자체만으로는 주 사업장을 결정하는 요소가 될 수 없으므로, 이는 주 사업장을 결정하는 기준이 아니다. 수탁처리자의 주 사업장은 수탁처리자의 유럽연합 내 중앙행정 지점이거나, 유럽 내 중앙 행정처리가 이루어지지 않는 경우에는 유럽연합 내 주요 처리 활동의 일어나는 장소가 주 사업장이다. 정보처리자와 수탁처리자 모두와 관련되어 있는 경우, 선임 감독기관은 처리자의 주 사업장이 있는 회원국의 감독기관이어야 하고 수탁처리자의 감독기관은 관련 감독기관으로 간주되어야 하며, 이 감독기관은 이 법에 규정된 협력 절차에 참여해야 한다. 어느 경우든, 수탁처리자의 단일 또는 복수의 사업장이 소재한 회원국 또는 복수의 회원국의 감독기관들은, 결정문 초안이 처리자에 한하여 관련되어 있는 경우, 관련 감독기관으로 간주되지 않는다. 사업체집단이 처리를 수행하는 경우, 통제 사업체의 주 사업장은 사업체집단의 주 사업장로 간주되어야하며, 처리 목적과 수단을 다른 사업체가 결정하는 경우는 예외로 한다.

(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

(37) 사업체그룹(a group of undertakings)은 관리하는 사업체와 관리되는 사업체를 포함하며, 관리하는 사업체는 소유권, 재정적 참여 또는 이를 관할하는 규정이나 개인정보보호 규정의 이행권한 등을 통해 다른 사업체에 우세적인 영향력을 행사할 수 있어야 한다. 부속 사업체 내의 개인정보 처리를 통제하는 사업체는 다른 사업체와 함께 사업체그룹으로 간주되어야 한다.

group of undertakings.

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

(38) 아동은 개인정보 처리에 따른 위험성, 결과, 이에 필요한 안전장치 및 본인의 권리를 잘 인지하지 못하고 있기 때문에 본인의 개인정보와 관련하여 구체적인 보호를 받아야 한다. 구체적인 보호는 특히 마케팅목적이나 사용자 프로필(user profiles) 혹은 가성인격을 만드는 목적으로 아동의 개인정보를 사용하는 경우와 아동에게 직접 제공되는 서비스를 이용하는 것과 관련하여 아동의 개인정보를 수집하는 경우에 적용되어야 한다. 아동에게 직접 제공되는 카운슬링이나 아동 보호서비스가 목적에는 양육책임자의 동의가 필수적이지 않다.

(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) 모든 개인정보처리는 합법적이고 공정해야 한다. 개인 본인과 관련된 개인정보가 수집, 이용, 참고정보로 활용되거나 혹은 다른 방식으로 처리된다는 사실, 그리고 어느 범위까지 그 정보가 처리되거나 처리될 것인지가 투명해야 한다. 이러한 투명성 원칙은 개인정보 처리와 관련하여 행하는 고지(information) 및 연락(communication) 일체가 용이하고 이해하기 쉬우며 명확·평이한 언어로 행해져야 한다. 투명성 원칙은 정보처리자의 신원과 처리 목적에 대한 고지(information), 해당 개인에 대한 공정하고 투명한 정보처리를 보장하기 위한 추가적 통지(further information)와 처리되고 있는 정보에 대해 확인받고 연락받을 수 있는 개인의 권리(right to obtain confirmation and communication)를 포함한다. 개인은 개인정보 처리와 관련하여 어떠한 위험성, 규정, 안전조치 및 권리가 있으며 이러한 권리를 어떻게 행사할 수 있는지에 대해서도 인지할 수 있도록 통지받아야 한다. 특히, 개인정보 처리에 관한 구체적인 목적은 명백하고 합법적이어야 하며, 개인정보 수집 당시에 결정되어야 한다. 개인정보 처리는 그 목적이 적절하고 연관성이 있어야 하고, 목적에 필요한 만큼에 한하야 제한되어야만 한다. 특히 개인정보 보관기간은 최소한으로 엄격하게 제한되어야 한다. 개인정보는 처리 목적이 여타 수단에 의해서는 합리적으로 성취될 수 없는 경우에 한하여 처리 될 수 있다. 정보처리자는 개인정보가 필요 이상으로 보관되지 않기 위해서 시간 한도를 설정해 두어야 하는데, 이를 통하여 정보처리자는 정보를 삭제하거나 주기적으로 확인(periodic review)할 수 있다. 부적절한 개인정보에 대한 수정 또는 삭제를 보장하는 모든 합리적인 조치가 취해져야 한다. 개인정보는 적절한 안정성(appropriate security)과 비밀(confidentiailty)을 보장하는 방식으로 처리되어야 하며, 이 방식에는 개인정보를 무단 열람·이용하려고 하는 것을 막고, 이를 위하여 사용되는 기기를 접근하지 못하도록 방지하는 방법 등이 있다.

(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

(40) 개인정보의 합법적인 처리를 위해서는, 정보주체의 동의를 근거로 하거나, 이 법 또는 이 법에 명시된 유럽연합·회원국 법률에 규정되어 있는 여타 합법적 근거를 기반으로 하여야 한다. 여타 합법적 근거로는, 정보처리자에게 부과된 법적 의무를 준수해야 한다는 것, 정보주체가 계약 당사자가 되는 계약 또는 계약 체결 전에 정보주체가 요구하는 사항을 이행해야 한다는 것 등이다.

a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

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

(41) 이 법에서 법적 근거나 법적 조치를 규정하고 있는 경우, 이 규정들이 회원국 의회의 입법과정을 거쳐 채택된 것일 필요는 없으며, 회원국의 헌법적 질서에 따른 필수사항들을 방해하지 않는다.(회원국의 입법과정을 거치지 않아도 되고 회원국 헌법 질서와 병립도 가능하다.) 단, 이러한 법적 근거 또는 법적 조치는 명확·상세하여야 하고, 법의 적용 대상인 개인이 유럽연합재판소와 유럽인권재판소의 판례법에 따라 그 적용을 예측할 수 있어야 한다.

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

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

(42) 개인정보 처리가 정보주체의 동의에 근거하는 경우, 정보처리자는 정보주체가 처리 방식에 대해 동의를 제공하였음을 입증할 수 있어야 한다. 특히 처리되는 사안이 아닌 다른 사안에 대해 서면 진술로 동의하는 경우, 정보주체가 어떤 정보가 어떤 범위로 제공된다는 사실을 인지할 수 있도록 보장하여야 한다. 유럽의회 지침 93/13/EEC1에 따라, 정보처리자가 제공하는 사전동의서 서식은 명확·평이한 언어를 사용하여 이해하기 쉽고, 열람이 가능하도록 하여야 하며 불공정한 용어를 포함해서는 안된다. 동의를 고지 받기 위해서는 정보주체는 최소한 정보처리자의 신원과 개인정보 처리 목적에 대해 인지하고 있어야 한다. 정보주체가 진심으로 동의하지 않았다거나, 자유로운 선택으로 동의하지 않았다거나, 손실 없이는 동의를 거절하거나 철회할 수 없는 경우에는 해당 동의는 자유롭게 제공된 것이라고 간주되지 않는다.

(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) 동의가 자유롭게 제공되기 위해서는, 정보주체와 정보처리자 간의 명백한 불균형이 존재하는 특정 상황과 같은 경우에는 동의를 합법적인 근거로 제시해서는 안된다. 특정상황이란 특히 정보처리자가 공공기관이기 때문에 동의가 자유롭게 제공될 것 같지 않은 경우이다. 개별적인 사례에서 적절하다고 판단되는 경우도 있겠으나, 별개의 개인정보 처리행위에 대해 별도의 동의를 받지 않는 경우이거나, 서비스 제공 등의 계약의 이행이 동의없이 이루어질 수 있음에도 불구하고 동의에 근거하여 진행되는 경우에는 해당 동의는 자유롭게 제공된 것이라고 볼 수 없다.

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

(44) 개인정보처리는 계약자체 또는 계약을 체결하기 위하여 필수적인 경우에 합법적이다.

(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

(45) 정보처리자에게 주어진 법적 의무에 따라 이행되거나 공익 또는 공적 권한으로 직무를 수행하는 과정에서 개인정보처리가 필요한 경우, 해당 정보처리는 유럽연합·회원국 법률에 근거가 있어야 한다. 이 법은

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.

각각의 정보처리에 대하여 구체적인 법률이 필요하다고 요구하는 것은 아니다. 정보처리자에게 적용된 법적 의무에 따른 복수의 처리방식에 대한 근거로써 또는 공익 또는 공적 권한의 행사를 위한 직무의 수행을 위해 개인정보처리가 필요한 경우, 하나의 법으로 충분하다. 또한 유럽연합법·회원국 법률은 처리목적을 결정할 수 있어야 한다. 유럽연합법·회원국 법률에서는 개인정보처리의 합법성을 관할하는 이 법의 일반적인 조건을 규정할 수 있고, 합법적이고 공정한 처리를 보장하기 위해 정보처리자, 해당 처리대상인 개인정보의 유형, 관련 정보주체, 해당 개인정보를 제공받는 기관, 목적제한, 보관기간과 기타 조치를 결정하는 세부사항을 수립할 수 있다. 또한 유럽연합법률 또는 회원국 법률은 공익 또는 공적 권한 행사에 따른 업무를 이행하는 관리자가 공법에 적용받는 공공기관이나 또 다른 개인 혹은 법인이어야 하는지, 공중보건, 사회보호, 의료서비스 관리 등 건강목적을 포함해 공익에 부합하는 경우, 전문가협회 등 민법에 적용 받는 지 결정할 수 있다.

(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) 개인정보의 처리는 정보주체의 생명 또는 또 다른 개인의 생명과 관련한 주요 이익을 보호하기 위하여 필요한 경우 합법적으로 간주된다. 타인의 생명과 관련한 주요 이익에 근거한 개인정보처리는 원칙적으로 해당 처리가 명백하게 다른 법적 근거에 기반 할 수 없는 경우에 한해서 행해져야 한다. 일부 정보처리 유형은 공익상 중요한 근거와 정보주체의 생명에 관련된 이익에 동시에 기여할 수도 있는데, 그 예로는 인도주의적 목적으로, 전염병과 확산에 대한 감시를 하거나 자연재해나 인재 등 인도적 비상사태 등에 처리가 필요한 경우가 있다.

(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

(47) 개인정보를 제공받을 수 있는 컨트롤러의 정당한 이익이나 제3자의 정당한 이익 등 컨트롤러의 정당한 이익은 처리의 법적 근거가 될 수 있다. 다만 컨트롤러와의 관계를 기반으로 정보주체가 합리적으로 예상하는 바를 고려하여 정보주체의 이익 또는 기본권 및 자유가 우선시되지 않는 경우에 한하여 그러하다. 이러한 정당한 이익은 정보주체가 컨트롤러의 고객이거나 컨트롤러의 서비스를 이용 중인 경우 등 정보주체와 컨트롤러 간에 타당하고 적절한 관계가 있을 때 존재할 수 있다. 어떠한 경우에든 정당한 이익의 존재에 대해서는 정보주체가 정보수집의 시점 및 정보수집의 상황에서 이러한 목적으로 정보가 처리될 수 있을 것이라고 합리적으로 예상할 수 있는지 여부 등에 관한 신중한 평가가 필요하다. 정보주체의 이익과 기본권은 특히 정보주체가 추가적 개인정보 처리에 대해 합리적인 예상을 하지 못한 상황에서 개인정보가 처리되는 경우 컨트롤러의 이익에 우선할 수 있다. 공공기관이 개인정보를 처리하는 법적 근거는 입법기관(the legislator)이 법률로써 규정한다는 점을 고려하면 공공기관이 본연의 업무를 수행할 때 발생하는 처리에는 해당 법적 근거가 적용되지 않는다. 사기 방지의 목적으로 반드시 필요한 처리 또한 해당 컨트롤러의 정당한 이익에 해당한다. 직접 마케팅(direct marketing)을 목적으로 하는 개인정보의 처

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.

리는 정당한 이익을 위해 시행된 것으로 간주될 수 있다.

(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) 사업체 집단 또는 중앙기구의 부속 기관의 일부인 컨트롤러는 고객이나 피고용인의 개인정보의 처리 등 내부 행정의 목적으로 사업체 집단 내에서 개인정보를 전송하는 정당한 이익을 가질 수 있다. 사업체 집단 내에서 제3국에 소재한 사업체로의 개인정보를 규정한 일반 원칙에는 적용되지 않는다.

(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) 오로지 네트워크 및 정보보안을 담보할 목적에 대하여 필요하고 비례하는 범위 내에서 이루어지는 개인정보의 처리는 관련 컨트롤러의 정당한 이익이 된다. 네트워크 및 정보보안이란 주어진 신뢰수준에서 네트워크나 정보시스템이 저장되거나 전송된 개인정보의 가용성, 진위성, 무결성, 기밀성을 해치는 우발적 사건이나 불법적 또는 악의적 행위에 저항하는 능력, 그리고 해당 네트워크와 시스템이 제공하거나 이를 통해 공공기관, 컴퓨터 비상 대응팀, 컴퓨터 보안사고 대응팀, 전자통신 네트워크·서비스 공급자, 보안기술·서비스 공급자가 제공받는 관련 서비스의 보안을 가리킨다. 여기에는 전자통신 네트워크에의 무단 접근 및 악성코드 배포를 방지하고 '서비스 거절' 공격 및 컴퓨터·전자통신시스템의 손상을 중지시키는 것이 포함될 수 있다.

(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

(50) 원래 수집 목적 이외의 개인정보 처리는 해당 개인정보의 처리가 원래의 수집 목적과 양립 가능한(compatible) 경우에 한해서만 허용되어야 한다. 목적이 양립 가능한 경우, 당초 정보수집을 허용한 법적 근거 이외의 별도의 법적 근거는 불필요하다. (목적이 양립가능하다면 별다른 근거 없이도 추가적으로 정보처리가 가능하다.) 공익을 추구하거나 컨트롤러에게 내재된 공적권한을 행사하여 시행되는 직무 이행에 처리가 필요한 경우, 유럽연합 또는 회원국 법률은 추가 처리가 양립 가능하고 적법하다고 간주되는 직무 및 목적을 결정하여 명시할 수 있다. 공익상의 기록 보존 목적, 과학·역사 연구 목적 또는 통계 목적으로의 추가 처리는 양립 가능의 적법한 처리 작업으로 간주되어야 한다. 유럽연합 또는 회원국 법률이 규정하는 개인정보 처리의 법적 근거는 추가 처리의 법적 근거도 될 수가 있다. 추가 처리의 목적이 당초 개인정보의 수집 목적과 양립 가능한지 여부를 확인하기 위해 컨트롤러는 당초 처리의 적법성에 관한 모든 요건을 충족시킨 후 무엇보다 당초 수집목적과 추가 처리 목적 간의 연관성, 해당 개인정보가 수집될 때의 상황, 특히 정보주체가 컨트롤러와의 관계를 토대로 추가 사용에 대해 합리적으로 예상할 수 있는 바, 해당 개인정보의 성격, 예정된 추가 처리가 정보주체에게 미치는 결과, 당초 처리작업 및 추가 처리작업에 적절한 안전장치의 유무를 고려하여야 한다.

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.

컨트롤러가 목적의 양립가능성 여부와 상관없이 해당 개인정보를 추가적으로 처리할 수 있는 경우가 있는데, 첫째, 정보주체가 동의하였거나, 둘째, 민주사회에서의 일반적 공익의 중요한 목표를 보호하는데 필수적이고 비례적인 대책들을 포함하고 있는 유럽연합·회원국의 법률에 근거하여 처리가 이루어지는 경우이다. 어떤 경우에서도 본 규정이 정한 원칙을 준수하여야 하며, 추가 처리 목적과 더불어 (처리) 반대권 등 정보주체의 권리를 정보주체에게 통보하여야 한다. 컨트롤러가 발생 가능한 범죄행위나 공안의 위협을 입증하고 동일한 범죄행위나 위협에 관한 개별 또는 복수의 사례에서 관련 개인정보를 관계 당국에 전송하는 것은 컨트롤러가 추구하는 정당한 이익으로 간주되어야 한다. 그러나 해당 정보처리가 법적, 직무상 또는 기타 구속력 있는 기밀유지의 의무와 양립가능하지 않는 경우, 컨트롤러의 정당한 이익을 위한 정보의 전송 및 추가 처리는 금지되어야 한다.

(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

(51) 개인정보의 특성 상, 기본권과 자유와 관련해 특히 민감한 개인정보는 기본권 및 자유 침해의 리스크를 야기할 수 있기 때문에 구체적인 보호를 받아야 한다. 이러한 정보에는 인종 또는 민족출신을 드러나는 개인정보도 포함되어야 하며, 이 법에서의 '인종출신'이라는 단어의 사용이 유럽연합이 인종을 분리하려는 이론을 용인한다는 의미가 아니다. 사진정보처리는 특정 개인 식별이나 인증 가능한 구체적인 기술적 수단을 통해 처리되는 경우에 한해서만 생체정보의 정의에 해당되기 때문에, 시스템적으로 민감처리로 분류되지 않는다. 이러한 개인정보는, 회원국의 법률이 공익 또는 정보처리자에게 부여된 공적 권한을 이행하기 위한 직무의 수행 또는 법적 의무의 준수를 위해 이 법의 규칙 적용을 변경하고자 개인정보에 대한 구체적인 조문을 규정할 수 있다는 사실을 고려하여 이 법에 따라 구체적인 상황에서 처리가 허용되는 경우가 아닌 이상, 처리되어서는 안된다. 이러한 처리에 대한 구체적인 요건과 함께, 이 법의 일반적인 원칙 및 기타 규정은 특히 합법적 처리를 위한 조건과 관련하여 적용되어야 한다. 특정 범주의 개인정보 등의 처리에 대한 일반적인 금지로부터의 일부 제외는 명백하게 제공되어야하는데, 특히 정보주체가 명백한 동의를 제공한 경우나 특별한 필요성이 있는 경우로, 특정 협회나 재단의 기본적 자유의 행사를 허용하는 목적으로 하는 합법적 활동과정에서 처리가 수행되는 경우 그러하다.

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.	
(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) 민감정보 처리를 금지한다는 일반적인 원칙은 유럽연합·회원국 법률에 규정되고 적절한 안전장치를 두고 있을 때 허용될 수 있다. 안전장치는 개인정보와 공익에 부합하는 기타 기본권을 보호하기 위한 것으로써, 특히 고용법, 연금과 사회보장 등 사회보호법, 감시(monitoring)와 경계(alert) 목적, 전염병과 기타 건강에 대한 심각한 위협을 예방하거나 통제하려는 목적일 경우이다. 민감정보 처리에 대한 예외적 허용은, 공중보건, 의료 서비스 관리 등 건강 목적을 위해 허용될 수 있으며, 특히 건강보험 제도상 청구절차가 그 혜택·서비스로 이어지는 과정에서의 품질 및 비용대비 효과를 보장하기 위해서나, 또는 공익적인 기록보존 목적, 과학 및 역사연구 목적 또는 통계목적을 위해 허용될 수 있다. 법적 청구권(legal claims)을 입증·행사하거나 방어할 때 필요한 경우 이러한 민감 정보를 허용할 수 있어야 하는데, 법원 내부에서의 절차나 행정절차 혹은 법원 외부 절차에 상관없이 가능하다.
(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) 더 높은 수준의 보호를 받아야 하는 특정범주의 개인정보는 건강관련 목적에 한해 처리되어야하며, 개인과 사회 전체의 이익을 위해 해당 목적을 성취하는데 필요한 경우 그러하다. 특히, 품질관리, 경영정보, 의료 및 사회보장시스템에 대한 일반적인 국가 및 지역적 감시의 목적, 건강 또는 사회보장의 연속성과 회원국 간 건강보험과 건강안전성을 보장하고, 감시 감독 목적으로 또는 공익적인 기록보존 목적, 과학 및 역사연구 목적 또는 통계 목적을 위하여, 이러한 데이터의 관리 및 중앙국립건강당국에 의해 처리되는 경우에 그러하다. 따라서 이 법은 이러한 개인정보의 처리가 직무상 기밀이란 법적 의무에 적용받는 개인에 의해 특정한 건강관련 목적으로 처리되는 경우 등, 구체적인 필요성과 관련하여 건강에 대한 특정범주의 개인정보 처리를 위한 통일된 조건을 규정해야 한다. 유럽연합 또는 회원국의 법률은 개인의 개인정보와 기본권을 보호하기 위해 구체적이고 알맞은 조치를 규정해야 한다. 회원국은 제한 등, 유전자 정보, 생체정보 또는 건강관련 정보처리와 관련한 추가적 조건을 유지 또는 도입하도록 허용되어야 한다. 그러나 이러한 조건이 회원국 간의 해당 정보처리에 적용될 때, 유럽연합 내 개인정보의 자유로운 흐름을 방해해서는 안된다.

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

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

(54) 특정범주의 개인정보처리는 정보주체의 동의 없이 공중보건 분야에서 공익 상의 이유로 필요할 수 있다. 이러한 처리는 개인의 권리와 자유를 보호하기 위해 적절하고 구체적인 조치를 적용받아야 한다. 이러한 상황에서, '공중 보건'은 유럽의회와 각료이사회의 규정(EC) No1338/2008에 정의에 따라 해석되어야 한다. 즉, 건강과 관련된 모든 요소로 질병 상황이나 장애 등의 건강상태, 이러한 건강상태에 영향을 미치는 결정적 요소, 의료보호서비스의 필요성, 의료보호서비스에 할당된 자원, 이에 대한 지출과 재정, 의료보호서비스 제공 및 보편적 이용, 그리고 사망 사유 등을 의미한다. 공익 상의 이러한 건강 관련 개인정보의 처리는 고용인 또는 보험사와 금융사 등 제 3자가 기타목적으로 개인정보를 처리하는 결과를 초래하지 않아야 한다.

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

(55) 또한 공공당국이 수행하는, 공인된 종교연합의 헌법 또는 국제공법으로 규정된 목표를 이루고자하는 목적의 개인정보처리는 공익을 이유로 수행된다.

(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) 선거활동의 경우, 회원국 내의 민주적 시스템의 운영은 정당이 개인의 정견에 대한 개인정보를 모으고, 이러한 개인정보의 처리는, 적절한 안전조치가 수립된 경우, 공익을 이유로 허용될 수 있음을 요구한다.

(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.

(57) 정보처리자가 본인이 처리하는 개인정보를 통해 개인을 식별하도록 허용하지 않는 경우, 정보처리자는 이 법의 모든 조항을 준수하는 유일한 목적을 위해 정보주체의 식별을 위한 추가정보를 획득하지 않아도 된다. 그러나 정보처리자는 정보주체가 본인의 권리의 행사를 지원하기 위해 추가정보를 제공하는 경우, 이를 받는 것을 거절하면 안된다. 식별에는 정보주체의 디지털 신원이 포함되어야 하며, 일례로 정보처리자가 제공하는 온라인 서비스에 정보주체가 로그인하기 위해 사용되는 동일한 증명서(credentials)와 같은 인증메커니즘을 통한 방법이 있다.

(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

(58) 투명성의 원칙에 따라 대중 또는 정보주체를 대상으로 한 일체의 통지는 간결하고 이용이 용이하며 이해하기 쉬워야 하고 명확하고 쉬운 언어가 사용되고, 추가적으로 적절한 경우 시각화 기법을 활용해야한다. 이러한 통지는 대중에게 제공될 경우 웹사이트를 통해 전자 양식으로 제공될 수 있다. 이는 온라인 광고 등, 많은 숫자의 활동주체 및 관행적인 기술적 복잡성으로 인해 정보주체가 본인의 개인정보가 누구에 의해 어떤 목적으로 수집되는지 파악하기 어려운 경우와 특히 관련이

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.

있다. 아동에게 특정한 보호수단이 필요하다는 것을 고려할 때 아동을 대상으로 한 정보처리의 경우 모든 통지 및 의사표시는 해당 아동이 쉽게 이해할 수 있는 명확하고 쉬운 언어가 이용되어야 한다.

(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) 이 법에 따라 정보주체의 권리의 행사 및 반대할 권리를 용이하게 하기 위해 양식(modalities)이 제공되어야하며 이 양식에는 개인정보에 대한 열람, 정정 또는 삭제 등을 요청하고, 가능한 경우, 무상으로 획득할 메커니즘이 포함된다. 정보처리자는 특히 전자적 수단으로 개인정보가 처리된 경우, 전자적인 양식의 요청을 위한 수단 또한 제공해야만 한다. 정보처리자는 과도한 지체 없이, 늦어도 한 달 이내에 정보주체의 요구에 대응해야하며 정보주체의 요구에 응하지 않으려는 경우, 그에 대한 이유를 제공해야할 의무가 있다.

(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) 공정하고 투명한 정보처리의 원칙에 따라 정보주체는 정보처리 방식의 존재와 및 그 목적에 대해 통지 받아야 한다. 정보처리자는 개인정보가 처리되는 구체적인 상황 및 맥락을 참작하여 공정하고 투명한 정보처리 보장에 필요한 모든 추가적인 정보를 정보주체에 제공해야 한다. 또한 정보주체는 프로파일링 유무와 해당 프로파일링의 결과에 대해 고지 받아야 한다. 정보주체로부터 개인정보가 수집되는 경우, 해당 정보주체는 본인이 개인정보 제공의 의무가 있는지의 여부 및 해당 정보를 제공하지 않을 경우의 결과에 대해 고지 받아야 한다. 정보주체에 제공되는 통지는 눈에 잘 띄고 이해하기 쉬우며 가독성이 뛰어난 방식으로 정보처리의 목적을 한 눈에 볼 수 있도록 표준화된 아이콘과 함께 제공될 수 있다. 전자 수단을 이용하여 아이콘을 제공하는 경우에는 기계 판독이 가능해야 한다.

(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) 정보주체에 대한 개인정보의 처리에 대한 통지는 정보수집 당시 정보주체로부터 또는 제3의 출처로부터 정보가 수집된 경우 적절한 기간 내에, 해당 경우의 상황에 따라, 정보주체에 제공되어야 한다. 개인정보가 합법적으로 제3의 수신인에게 제공될 수 있는 경우, 해당 정보주체는 정보가 처음 해당 수신인에게 제공될 시 이를 고지 받아야 한다. 정보처리자가 당초 정보수집 목적 이외의 목적으로 개인정보를 처리하려는 경우, 정보처리자는 추가 정보처리에 앞서 정보주체에게 해당 목적에 대한 정보 및 기타 필요한 정보를 제공해야 한다. 다양한 출처의 활용으로 인해 정보주체에게 개인정보의 출처를 제공할 수 없는 경우, 일반적인 통지가 제공되어야 한다.

(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) 그러나 정보주체가 이미 해당 통지사항을 보유한 경우, 법률이 해당 개인정보의 기록 또는 제공을 명백히 규정한 경우, 정보주체에 해당 통지를 제공하는 것이 불가능하거나 여기에 과도한 노력이 요구되는 경우, 본 의무를 부과할 필요가 없다. 후자는 공익적인 기록보존 목적, 또는 과학 및 역사적 연구 목적, 또는 통계목적으로 정보가 처리되는 경우가 해당될 수 있다. 이와 관련해 정보주체의 인원수, 해당 개인정보의 생성시점 및 채택된 모든 적절한 보호수단이 고려될 수 있다.

(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) 정보주체는 개인정보 처리의 적법성을 인지하고 검증하기 위해 본인과 관련해 수집된 개인정보를 열람할 권리 및 이 권리를 용이하게 적절한 시간적 간격으로 행사할 수 있는 권리를 가진다. 여기에는 개인이 본인의 건강, 예를 들어 진단, 검사 결과, 담당 의사의 평가 및 행해진 치료 또는 조치 등의 정보가 담긴 의료기록의 정보와 관련한 건강관련 개인정보를 열람할 수 있는 권리도 포함된다. 따라서 모든 정보주체는 특히 개인정보가 처리되는 목적, 가능한 경우 처리기간, 개인정보의 수신인, 자동개인정보처리에 수반된 논리, 최소한 프로파일링을 근거로 한 해당 정보처리의 결과에 대해 알고 소통할 수 있는 권리를 가진다. 가능한 경우, 정보처리자는 정보주체가 본인의 개인정보를 직접 열람할 수 있는 보안시스템에 원격 접속 가능하도록 할 수 있다. 이 권리가 사업상 기밀 또는 지적재산권 및 특히 소프트웨어 보호 저작권 등 타인의 권리 및 자유에 악영향을 끼쳐서는 안 된다. 그러나 상기 사항을 고려함으로 인해 정보주체에 이에 관한 통지를 제공하는 것이 거부되어서는 안 된다. 정보처리자가 정보주체에 관해 대량의 정보를 처리하는 경우, 정보처리자는 해당 통지를 전달하기 전에 정보주체가 해당 요청에 관계된 통지 또는 처리 활동을 구체적으로 명시하도록 요구할 수 있다.

(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) 정보처리자는 특히 온라인서비스 및 온라인 식별자와 관련한 상황에서 개인정보 열람을 요구한 정보주체의 신원을 확인하기 위해 모든 합당한 조치를 취해야 한다. 정보처리자는 잠재적 요청의 응대라는 유일한 목적만으로 개인정보를 보유해서는 안 된다.

(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

(65) 정보주체는 본인의 개인정보의 보유가 이 법이나 정보처리자에 적용되는 유럽연합 또는 회원국 법률을 침해하는 경우, 본인에 대한 개인정보를 정정할 권리와 '잊힐 권리'를 가져야 한다. 특히 정보주체는 본인의 개인정보를 삭제할 권리와 해당 정보가 더 이상 처리되지 않게 할 권리를 가져야 하며, 이에 해당하는 경우에는 해당 개인정보가 당초 수집 목적과 관련하여 더 이상 필요 없거나 다르게 처리되는 경우, 정

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.

보주체가 본인의 동의를 철회하거나 본인에 관한 개인정보의 처리에 반대하는 경우, 또는 본인의 개인정보의 처리가 다르게 처리되면 이 법을 준수하지 않을 경우가 있다. 상기 권리는, 특히 정보주체가 아동으로서 본인의 동의를 제공하고, 처리에 관한 리스크를 완전히 인지하지 못하고 이후 특히 인터넷 상에서 이러한 개인정보를 지우고 싶어 하는 경우와 관련 있다. 해당 정보주체가 더 이상 어린이가 아닐지라도 이 권리를 행사할 수 있어야 한다. 그러나 개인정보의 추가적 보유는 필요한 경우 적법하며, 여기에는 표현 및 정보의 자유권 행사, 법적 의무 준수, 공익 또는 정보처리자에 부여된 공적 권한 행사를 위해 시행되는 직무 수행, 공중 보건 분야의 공익상의 이유와, 공익적인 기록보존목적, 과학 및 역사적 연구목적 또는 통계목적, 법적 청구권 입증, 행사 및 방어를 위한 경우가 해당한다.

(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) 온라인 환경에서 잊힐 권리를 강화하기 위해서 개인정보를 공개한 관리자가 해당 개인정보를 처리한 관련 관리자에게 해당 개인정보에 대한 링크, 사본, 재현물을 삭제할 것을 고지할 의무를 지니게 하는 방식으로 삭제할 권리를 확대해야 한다. 이렇게 하기 위해서, 해당 관리자는 해당 개인정보를 처리한 다른 관리자에게 정보주체의 요청사항을 통지하기 위해 기술 대책을 비롯한 가용할만한 기술 및 수단을 고려한 합리적인 조치를 취해야 한다.

(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) 개인정보 처리를 제한하는 방법에는 선택된 정보를 임시적으로 다른 처리 시스템으로 이전하거나, 이용자가 선택된 정보를 열람하지 못하게 하거나 공개된 개인정보를 웹사이트에서 임시로 제거하는 것이 포함될 수 있다. 개인정보처리 제한은, 자동프로파일링 시스템에서 관련 개인정보에 추가적 처리방식이 적용되지 않고 변경되지 않는 방식으로 기술적인 수단에 의해 원칙적으로 보장되어야 한다. 개인정보 처리가 제한된다는 사실은 시스템에 명백하게 표시되어야 한다.

(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

(68) 자동수단을 통해 개인정보가 처리되는 경우, 정보주체 본인의 개인정보에 대한 통제권을 더욱 강화하기 위해 정보주체는 본인이 정보처리자에게 제공한 본인의 개인정보를 조직적이고 상용화된, 기계판독 및 상호호환이 가능한 형식으로 수령 받도록 허용되거나 이를 또 다른 관리자에게 이전할 수 있어야 한다. 정보처리자는 본인의 개인정보 이전(data portability)을 가능하게 하는 상호호환적인 포맷을 개발하도록 장려되어야 한다. 이러한 권리는 정보주체가 본인의 동의에 근거하여 또는 계약의 이행에 처리가 필요한 경우 개인정보를 제공했을 때 적용되어야 한다. 처리가 동의 또는 계약 이외의 법적 사유를 근거로 하는 경우에는 이 권리는 적용되지 않는다. 이 권리는 그 성격 상, 공적 업무 수행을 위해 개인정보를 처리하는 정보처리자에 반(反)하여 행사되어서는 안된다. 따라서 정보처리자가 적용받는 법적의무를 준수하기

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.

위해 또는 공익이나 정보처리자에게 부여된 공적권한의 행사를 위한 직무의 수행에 개인정보가 필요한 경우에는 이 권리가 적용되어서는 안된다. 본인의 개인정보 수령 또는 이전하는 정보주체의 권리가 정보처리자가 기술적으로 양립 가능한 처리 시스템을 채택 또는 유지하도하는 의무를 생성해서는 안된다. 특정 개인정보 세트에 복수의 정보주체가 관련되는 경우, 개인정보를 수령 받을 권리는 이 법에 따라 다른 정보주체의 권리와 자유를 침해해서는 안된다. 또한 이 권리는 정보주체가 본인의 개인정보를 삭제할 권리와 이 법에서 규정하는 이 권리에 대한 제한을 침해해서도 안되며, 특히 이 권리는 계약의 이행의 범위에 해당하는 만큼 그리고 계약의 이행에 개인정보가 필요한 기간 동안 정보주체가 제공한 본인의 개인정보에 대한 삭제를 의미하지 않는다. 기술적으로 가능한 경우, 정보주체는 해당 개인정보를 한 정보처리자에서 또 다른 정보처리자로 직접 이전할 수 있는 권리를 가진다.

(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) 공익을 추구하거나 컨트롤러에 부여된 공적 권한을 행사하여 또는 컨트롤러나 제3자의 정당한 이익에 근거하여 처리가 필요한 이유로써 개인정보의 처리가 적법할 수 있는 경우, 정보주체는 그럼에도 불구하고 본인의 특정 상황과 관련한 어떤 개인정보의 처리에라도 반대할 권한이 있다. 컨트롤러가 가지는 설득력 있는 정당한 이익이 정보주체의 이익이나 기본권 및 자유에 우선한다는 것을 입증하는 것은 컨트롤러의 책임이다.

(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) 직접 마케팅을 목적으로 개인정보를 처리하는 경우, 정보주체는 최초 또는 추가처리와 관련 있는 지 여부와 상관없이, 이러한 직접 마케팅과 관련한 범위에 해당하는 프로파일링 등, 이러한 처리에 대해 언제든지 무상으로 반대할 권리를 갖는다. 이 권리는 정보주체가 명백하게 인지할 수 있도록 제공되어야 하며 다른 기타 정보와는 별도로 명백하게 제시되어야 한다.

(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

(71) 정보주체는 자동처리에만 근거하여 정보주체의 개인적인 측면을 평가하는 조치를 포함할 수 있고, 온라인 신용신청에 대한 자동적 거절이나 인적개입 없이 이루어지는 전자채용 관행 등 정보주체에게 법적인 영향이나 이에 상응하는 중대한 영향을 미치는 결정에 적용받지 않을 권리를 갖는다. 이러한 처리는, 개인의 개인적인 측면을 평가하는 모든 형태의 개인정보의 자동처리로 구성된 '프로파일링'을 포함하며, 특히 정보주체의 업무능력, 경제적 상황, 건강, 개인의 성향이나 관심사, 신뢰성 또는 행동, 위치 또는 움직임과 관련된 측면을 분석하고 예측하며, 정보주체에게 법적인 영향이나 이에 상응하는 중대한 영향을 미치는 경우 그러하다. 그러나 프로파일링 등 이러한 처리에 근거한 의

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.

사결정은, 정보처리자가 적용받는 유럽연합 또는 회원국의 법률에서 명시적으로 인가하는 경우 허용되어야하며, 여기에는 사기 및 탈세의 감시목적과 이 법 및 유럽연합기구와 국가 감시기구의 기준 및 권고책에 따른 예방 목적이 포함되며, 정보처리자가 제공하는 서비스의 보안과 안정성을 보장하고, 정보주체와 정보처리자 간의 계약의 체결이나 수행에 필요한 경우, 또는 정보주체가 본인의 명백한 동의를 제공하는 경우가 해당한다. 어떠한 경우에도, 이러한 처리는 정보주체에게 구체적인 통지전달, 인적개입을 획득할 수 있는 권리, 의사를 표현할 권리, 이러한 평가 이후 도달한 결정에 대한 설명을 획득할 권리, 해당 결정에 이의를 제기할 권리 등, 적절한 안전조치를 적용받아야 한다. 이러한 조치에 아동은 해당하지 않는다.

정보주체와 관련하여 공정하고 투명한 처리를 보장하기 위해서, 개인정보가 처리되는 특정한 환경과 상황을 고려하여, 정보처리자는 프로파일링을 위한 적절한 수학적 또는 통계적 절차를 사용해야하며, 특히 개인정보의 부정확함을 초래할 수 있는 요소를 시정하고 오류의 위험성의 최소화를 보장하기 위해 기술 및 관리조치가 이행되어야하며, 개인정보를 정보주체의 이익과 권리를 위해 관련된 잠재적 위험요소를 고려하는 방식으로, 특히 개인의 인종 또는 민족출신, 정견, 종교나 신념, 노동조합의 가입여부, 유전적 또는 건강상태나 성적취향에 근거하여 개인에 미치는 차별을 방지하는 방식이나 이러한 영향을 지니는 조치를 초래할 수 있는 방식으로 보호해야 한다. 자동적 의사결정과 특정범주의 개인정보에 근거한 프로파일링은 특정 조건에 한해서만 허용되어야 한다.

(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) 프로파일링은 처리원칙 또는 개인정보보호 원칙을 위한 법적 근거 등, 개인정보의 처리와 관련한 이 법의 규칙을 적용받는다. 이 법에 따라 설립된 유럽의 개인정보보호 이사회('이사회')은 이러한 맥락에서 지침을 발간할 수 있어야 한다.

(73) Restrictions concerning specific principles and concerning the rights of information, access to and rectification or erasure of personal data and on the right to data portability, the right to object, decisions based on profiling, as well as on the communication of a personal data breach to a data subject and on 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 man made disasters, the prevention, investigation and prosecution of criminal offences or the

(73) 특정 원칙과 통지권, 개인정보의 열람권, 수정 또는 삭제권, 본인의 정보이동권(the right to data portability), 반대할 권리, 프로파일링에 근거한 결정 및 개인정보의 유출에 대한 정보주체로의 통지와 정보처리자의 특정 관련 의무에 대한 제한은 유럽연합 또는 회원국의 법률에 따라 민주주의 사회에서 유럽연합 또는 회원국의 법률에 따라 다음을 위해, 즉, 생명의 보호 등, 특히 자연재해나 인재에 대응하고, 공안에 대한 위협과 규제받는 직업적 윤리의 침해로부터의 보호 및 방지 등, 범죄 예방, 조사 및 기소나 형사 처분의 수행 등 공안을 보호하기 위해, 유럽연합 또는 회원국의 일반적인 공익상의 중요한 기타 목적, 특히 유럽연합 또는 회원국의 중요한 경제적 또는 재정적 이익을 보호하고 공개등록부(public registers)를 일반적인 공익 상의 이유로 기록을

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.	보호하며, 보관된 개인정보를 이전의 전체주의 정권 하의 정치적 행동에 관련한 특정 정보를 제공하기 위한 추가적 처리를 보호하거나, 사회적 보호, 공중보건이나 인도적 목적 등, 정보주체 또는 제 3자의 권리와 자유를 보호하는데 필요하고 비례하는 수준에서 부과될 수 있다.
(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) 개인정보 정보처리자 또는 정보처리자를 대신하여 개인정보처리를 수행하는 정보처리자에 대한 책임(responsibility and liability)이 수립되어야 한다. 특히 정보처리자는 적절하고 효과적인 조치를 시행할 의무를 지녀야하며 시행한 조치의 효과를 포함하여 이 법을 준수하여 처리활동을 하고 있음을 입증할 수 있어야 한다. 이러한 조치는 개인정보처리의 성격, 범위, 상황, 목적 그리고 개인의 권리와 자유에 관한 위험요소를 고려해야 한다.
(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) 자연인의 권리와 자유에 미치는 위험성은 그 발생가능성 및 중대성은 다르나 개인정보 처리로부터 초래될 수 있으며, 이는 신체적, 물질적, 비(非) 물질적 피해로 이어질 수 있다. 특히 처리로 인해 차별, 신용도용, 신용사기, 재정적 손실, 명예 훼손, 직무상 기밀로 보호되던 개인정보의 기밀성 상실, 가명처리에 대한 무단 재식별처리, 기타의 심각한 경제적 또는 사회적 불이익을 초래할 수 있는 경우, 정보주체가 본인의 권리와 자유를 박탈당할 수 있는 경우, 개인정보가 인종·민족 출신, 정견, 종교·철학적 신념, 노동조합의 가입여부, 유전자 정보, 건강 관련 정보, 성생활이나 유죄판결·형사범죄 관련 정보의 처리 또는 관련 보안조치를 드러내는 방식으로 처리되는 경우, 개인의 프로필 생성 또는 활용을 위해 개인적 측면, 특히 업무 성과, 경제적 상황, 건강, 개인의 선호 및 관심사, 신뢰성 또는 행태, 위치 또는 이동에 관한 측면을 분석 또는 예측하여 평가하는 경우, 아동 등 취약한 자연인의 개인정보가 처리되는 경우, 처리가 방대한 양의 개인정보와 관련되거나 다수의 정보주체에게 영향을 미치는 경우가 그러하다.
(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	(76) 정보주체의 권리와 자유에 대한 위험요소의 발생가능성과 심각성은 해당 처리의 성격, 범위, 상황 및 목적을 참고하여 결정되어야 한다. 위험성은 개인정보처리의 방식이 위험요소 또는 높은 수준의 위험요소와 관련 있는 지 여부를 입증하는 객관적인 평가에 근거하여 평가되어야 한다.

processing operations involve a risk or a high risk.

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

(77) 적절한 조치의 시행에 대한 지침과 처리의 위험요소의 확인, 위험요소의 출처, 성격, 가능성, 심각성을 고려한 평가 및 위험요소의 완화방침에 대한 확인과 관련하여 이 법을 준수하여 처리했음을 입증하는 지침은 특히, 인가된 행동강령 및 공인인증서, 이사회의 가이드라인을 통해 제공되거나 개인정보보호 담당관이 제공하는 지표를 통해 제공되어야 한다. 이사회는 개인의 권리와 자유에 관한 높은 수준의 위험요인을 초래할 가능성이 낮다고 간주되는 처리 방식에 대한 가이드라인을 발간할 수 있으며 이러한 위험요소를 해결하기 위해 충분한 조치가 무엇인지 표시할 수 있다.

(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) 개인정보의 처리와 관련하여 자연인의 권리와 자유를 보호하기 위해서는 적절한 기술적·관리적 조치를 시행함으로써 본 규정의 요건을 충족시켜야 한다. 본 규정의 준수를 입증하기 위해 컨트롤러는 특히 개인정보보호 최적화 설계 및 기본설정의 원칙을 충족시키는 내부 정책과 조치를 채택하고 시행하여야 한다. 그 같은 조치는 무엇보다 개인정보 처리의 최소화, 가능한 빠른 시일 내 적용되는 개인정보의 가명처리, 개인정보의 기능 및 처리에 관한 투명성으로 구성되고, 이를 통해 정보주체는 정보처리를 모니터링하고 컨트롤러는 보안을 확립 및 개선할 수 있다. 개인정보의 처리를 기반으로 하거나 작동 중에 개인정보를 처리하게 되는 애플리케이션·서비스·제품을 개발, 설계, 선택, 활용할 시, 해당 제품·서비스·애플리케이션의 생산자는 이를 개발하고 설계할 때 개인정보 보호 권리를 고려하고 최첨단 여부를 적절히 살펴 컨트롤러와 프로세서가 개인정보 보호의 의무를 준수할 수 있도록 보장해야 한다. 개인정보보호 최적화 설계 및 기본설정의 원칙은 공개입찰 시에도 고려되어야 한다.

(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) 정보주체의 권리와 자유에 대한 보호와 정보처리자 및 수탁처리자의 책임(responsibility and liability)은 감독기관의 감시 및 조치와도 관련하여 이 법에 따른 책임의 명확한 분배를 요구한다. 여기에는 정보처리자가 다른 정보처리자와 공동으로 개인정보처리의 수단과 목적을 결정하는 경우, 또는 정보처리자를 대신하여 처리방식이 수행되는 경우가 해당한다.

(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

(80) 유럽연합의 역외지역의 설립된 정보처리자 또는 수탁처리자는 유럽 내의 정보주체의 개인정보를 처리하고, 이러한 처리활동이, 정보주체에게 지불을 요청한 여부와 상관없이, 해당 정보주체에게 재화와 서비스를 제공하는 것과 관련 있는 경우, 또는 유럽 내에서 발생하는 정보주

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 the processor to act on its behalf with regard to their obligations under this Regulation. The designation of such representative does not affect the responsibility and liability of the controller or the processor under this Regulation. Such representative should perform its tasks according to the mandate received from the controller or processor, including to cooperate with the competent supervisory authorities on any action taken in ensuring compliance with this Regulation. The designated representative should be subject to enforcement proceedings in the event of non-compliance by the controller or processor.

체의 행동에 대한 감시와 관련 있는 경우, 해당 정보처리자 또는 수탁처리자는 대리인을 지정해야 하지만, 처리가 수시적이지 않고, 대규모의 처리나 특정범주의 개인정보의 처리, 또는 형사기소나 범죄에 관련된 개인정보의 처리가 포함되지 않은 경우, 그리고 처리의 성격, 상황, 범위 그리고 목적을 고려했을 때 개인의 권리와 자유에 관해 위험요소를 초래할 가능성이 낮은 경우나 정보처리자가 공공기관이나 기구인 경우에는 예외이다. 대리인은 정보처리자와 수탁처리자를 대신하여 행동해야 하며 어떠한 공공기관도 대리인을 지정할 수 있다. 대리인은 정보처리자 또는 수탁처리자의 공식 위임서한을 통해 명확하게 지정되어 이 법에 규정된 처리자들의 의무와 관련하여 대신 행동한다. 이러한 대리인의 지정은 이 법에 규정된 정보처리자 또는 수탁처리자의 책임(responsibility and liability)에는 영향을 미치지 않는다. 해당 대리인은 정보처리자에게 부여받은 권한에 따라 대리자로써의 업무를 수행해야하며, 여기에는 이 법을 준수하기 위해 적용된 모든 조치에 관해 관련 감독기관과 협력하는 것이 포함된다. 지정된 대리인은 정보처리자 또는 수탁처리자가 규정을 준수하지 않은 경우, 집행절차를 적용받아야 한다.

(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) 정보처리자를 대신한 수탁처리자 수행하는 처리와 관련하여 이 법을 준수하도록 보장하기 위해서, 수탁처리자에게 처리 활동을 위탁할 때, 정보처리자는 전문적 지식, 신뢰성 및 자원과 특히 관련하여, 처리의 보안 등, 이 법의 요건을 맞출 수 있는 기술 및 관리조치의 시행한다는 충분한 확신을 제공하는 수탁처리자만을 활용해야 한다. 수탁처리자의 승인된 행동강령이나 공인 인증메커니즘에 대한 준수는 정보처리자의 의무의 준수를 입증하는 요소로 이용될 수 있다. 수탁처리자의 개인정보처리의 수행은 유럽연합 또는 회원국 법률에 규정된 계약 또는 기타 법률에 적용받아야 하며, 이를 통해 수탁처리자는 정보처리자에게 구속되고, 처리 주제 및 처리기간, 처리의 성격 및 목적, 개인정보 유형 및 정보주체의 범주를 규정하며, 수행되는 개인정보처리의 상황에서의 수탁처리자의 구체적인 업무 및 책임과 정보주체의 권리와 자유에 대한 위험요소를 고려하게 된다. 정보처리자와 수탁처리자는 개별 계약을 선택하거나 위원회가 직접 채택하거나 감독기관이 일관성 메커니즘에 의거하여 채택 후 위원회가 다시 채택한 정보보호 표준계약조항(standard contractual clauses) 중 하나의 방식을 선택할 수 있다. 정보처리자를 대신하여 처리를 완료한 후, 수탁처리자는, 정보처리자의 선택에 따라, 관련 개인정보를 반환 또는 파기해야하지만, 수탁처리자가 적용받는 유럽연합 또는 회원국 법률에 따라 개인정보를 보관하라는 요구사항이 있는 경우는 예외로 한다.

(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) 이 법의 준수를 입증하기 위해, 정보처리자 또는 수탁처리자는 본인의 책임 하에 처리활동 기록을 유지해야한다. 각 정보처리자와 수탁처리자는 감독기관와 협동할 의무와 관련 기록을, 요청 시, 이용 가능하게 하여 처리활동을 감시하는데 사용할 의무가 있다.
(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 stateof 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) 보안을 유지하고 이 법을 위반하는 처리를 방지하기 위해서 정보처리자 또는 수탁처리자는 처리에 내재된 위험요소를 평가하고 암호처리 등, 해당 위험요소를 완화할 수 있는 조치를 시행해야 한다. 이러한 조치는 보호되어야 할 개인정보에 관한 위험요소 및 성격과 관련한 조치의 시행에 소요되는 비용 및 첨단 수준을 고려하여, 기밀성 등, 보안의 적절한 수준을 보장해야 한다. 개인정보의 보안위험요소를 평가할 때, 개인정보 처리로 인해 발생하는, 이전, 보관 또는 다른 방식으로 처리된 개인정보의 사고적 혹은 불법적 파기, 손실, 변경, 무단제공 등 특히 신체적, 물질적 그리고 비(非) 물질적 피해를 초래할 수 있는 위험요소를 고려해보아야 한다.
(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) 처리 방법이 개인의 권리와 자유에 관해 높은 수준의 위험요인을 초래할 가능성이 있는 경우 이 법을 보다 더 잘 준수하기 위해서, 정보처리자는 관련 위험요소의 출처, 성격, 특성 그리고 심각성을 특히 평가하는 개인정보보호 영향평가를 수행할 책임을 지녀야 한다. 평가의 결과는 개인정보의 처리가 이 법을 준수하였음을 입증하기 위해 취해지는 적절한 조치를 결정할 때에 고려되어져야 한다. 개인정보보호 영향평가에서 정보처리자가 가용할만한 기술과 이행의 비용 면에서 적절한 조치를 취해 완화할 수 없는 높은 수준의 위험요소가 처리방식에 포함되어 있다면 표시한다면, 감독기관의 자문이 처리 이전에 이루어져야 한다.
(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.	(85) 개인정보의 유출은, 적절하고 시의 적절하게 해결되지 않을 경우, 본인의 개인정보에 대한 통제권 상실이나 권리 제한, 차별, 신용도용 및 신용사기, 재정적 손실, 가명처리의 무단 재식별, 명예훼손, 직무상 비밀이던 개인정보의 기밀성 상실과 기타 경제적 또는 사회적 불이익 등과 같은 신체적, 물질적 그리고 비(非) 물질적 피해를 초래할 수 있다. 따라서 정보처리자는 개인정보 유출을 알게 되는 즉시 지체 없이 가능한 72시간 이내에 관련 감독기관에 이 사실을 고지하여야 한다. 그러나 정보처리자가, 책임성의 원칙에 따라, 해당 개인정보의 유출이 개인의 권리와 자유에 관해 위험요소를 초래할 가능성이 낮다고 입증할 수 있는 경우는 예외로 한다. 해당 유출사고의 통지가 72시간 이내에 이루어지지 않을 경우, 지체된 이유는 통지내용과 제공되고 관련 정보는 추가적 지체 없이 단계별로 제공될 수 있다.

Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay.

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

(86) 정보처리자는 개인정보의 유출이 개인의 권리와 자유에 관해 높은 수준의 위험요소를 초래할 가능성이 있는 경우, 정보주체가 필요한 예방조치를 취할 수 있도록 지체 없이 개인정보의 유출을 정보주체에게 고지해야 한다. 이러한 고지는 개인정보의 성격 및 잠재적 부작용을 완화하기 위한 개인에 대한 권고대책을 설명해야 한다. 이러한 고지는 합리적으로 가능한 빨리, 감독기관 또는 법집행기관 등 관련 기타 관련 기관이 제공하는 지침을 준수하며 해당 감독기관과의 긴밀한 협력 아래에 이루어져야 한다. 예를 들어, 즉각적인 피해의 위험성을 완화하고자 하는 경우, 즉각적인 정보주체로의 통지가 요구되는 한편, 지속적이거나 비슷한 개인정보의 유출을 막는 적절한 조치를 취하고자 하는 경우, 통지하기까지 소요되는 더 오랜 시간을 정당화 할 수 있다.

(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) 적절한 기술적 보호 및 관리조치가 개인정보의 유출의 발생여부를 즉각적으로 입증하고 이를 감독기관과 정보주체에 즉시 통지하기 위해 이행되었는지 여부를 확인해야 한다. 이러한 통지가 지체 없이 이루어졌다는 사실은, 특히 개인정보의 유출의 성격과 강도와, 정보주체에게 미치는 결과와 부작용에 대해 고려하여 입증되어야 한다. 이러한 통지는 이 법에 규정된 감독기관의 업무와 권위에 따라 감독기관의 개입을 초래할 수 있다.

(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) 개인정보의 유출에 대한 통지에 적용 가능한 형식과 절차에 관한 상세한 규정을 설정할 때, 적절한 기술적 보호조치를 통해, 신용사기 또는 다른 형태의 오용의 가능성을 효과적으로 제한하여, 개인정보가 보호될 수 있었는 지 여부 등 개인정보의 유출에 대한 상황이 충분히 고려되어야만 한다. 또한 이러한 규정 및 절차는, 조기제공이 유출상황에 대한 조사를 불필요하게 방해할 수 있는 경우, 법집행기관의 정당한 이익을 고려해야 한다.

(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

(89) 지침 95/46/EC에서는 개인정보의 처리를 감독기관에 통지하는 일반적인 의무사항을 규정하고 있다. 이러한 의무는 행정적, 재정적 부담이지만, 모든 경우에 개인정보의 보호를 개선하는 데 도움이 되는 것은 아니다. 이러한 무차별적인 일반적인 통지의 의무는, 따라서, 철폐되어야 하며, 대신 처리방식의 성격, 범위, 상황 및 목적을 기준으로 개인의 권리와 자유에 관한 위험요소를 초래할 수 있는 처리방식에 대응하는 효과적인 절차 및 메커니즘으로 대체해야 되어야 한다. 이런 유형의 처리방식은 특히 신기술의 이용과 관련 있거나, 새로운 종류의

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.

처리방식이거나, 정보처리자에 의한 개인정보보호 영향평가가 이루어지지 않았던 처리방식이거나 또는 최초의 처리 이후, 시간이 흘러 필요하게 된 경우일 수 있다.

(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) 이러한 경우, 개인정보보호 영향평가는 높은 수준의 위험 가능성 및 강도를 평가하기 위해 처리의 성격, 범위, 상황과 목적 그리고 위험요소의 출처를 고려하여, 처리 이전에 정보처리자에 의해 수행될 수 있어야 한다. 개인정보보호영향평가는 특히 해당 위험성을 완화하고 개인정보의 보호를 보장하며 이 법을 준수했음을 입증하는데 예상되는 조치, 안전장치 및 메커니즘을 포함해야 한다.

(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) 이는 특히 상당한 양의 개인정보를 지역적, 국가적, 초국가적 차원에서 처리하고자 하는 대규모의 처리방식과 수많은 정보주체에게 영향을 미칠 수 있는 처리방식, 그리고 현재의 기술적 지식의 수준에 따라 새로운 기술이 대규모 처리에 사용되어지는 경우 등, 그 민감성 때문에 높은 수준의 위험요소를 초래할 수 있는 처리방식뿐 아니라 정보주체가 그들의 권리를 행사하기 어려운 상황 등, 정보주체의 권리와 자유에 관해 높은 수준의 위험요소를 초래할 수 있는 기타 처리 방식에 적용되어야 한다. 개인정보보호 영향평가는, 또한, 개인정보가 특정 개인에 대한 결정을 내릴 때 처리되는 경우에 관련 개인정보의 프로파일링에 근거하여 개인에 관련된 개인적인 측면에 대한 체계적이고 광범위한 모든 평가를 따르거나 특별범주의 개인정보, 생체정보 또는 형사기소 및 범죄나 관련보안조치에 대한 정보의 처리를 따라 이루어져야 한다. 개인정보보호 영향평가는 특히 영상전자기기 사용 시, 공공장소에 대한 대규모 감시를 위해 또는 관련 감독기관이, 특히 정보주체가 권리를 행사하거나 서비스 또는 계약을 이용하지 못하게 되거나 체계적으로 대규모로 처리를 수행하여, 해당 처리가 정보주체의 권리와 자유에 관한 높은 수준의 위험요소를 초래할 가능성이 있다고 생각되는 경우, 모든 기타 처리 방식에 동등하게 요구되어 진다. 개인정보의 처리는 해당 처리가 개인 내과 의사나 기타 의료전문인 또는 변호사의 환자나 고객으로부터의 개인정보와 관련하는 경우, 대규모의 진행이 고려되어서는 안된다. 이러한 경우, 개인정보보호 영향평가는 의무사항이 아니다.

(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

(92) 개인정보보호영향평가의 대상이 하나의 프로젝트보다 광범위해야 합리적이고 경제적일 수 있다고 판단되는 상황에는 공공기관 또는 기구가 통일된 적용 또는 처리 플랫폼을 설립하려는 의도가 있는 경우, 또는 여러 명의 정보처리자가 하나의 산업분야나 부문의 전체에 또는 광범위한 활동에 통일된 적용 또는 처리환경을 도입하고자 계획하는 경우가 있다.

processing environment across an industry sector or segment or for a widely used horizontal activity.	
(93) In the context of the adoption of the Member State law on which the performance of the tasks of the public authority or public body is based and which regulates the specific processing operation or set of operations in question, Member States may deem it necessary to carry out such assessment prior to the processing activities.	(93) 공공기관 또는 공공기구의 업무 수행의 근간이 되고 특정 처리방식이나 해당되는 일련의 처리방식들을 규제하는 회원국의 법률을 채택하는 상황에서, 회원국은 처리 활동에 앞서 개인정보보호 영향 평가를 수행할 필요가 있다고 생각할 수 있다.
(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) 개인정보보호 영향평가는 해당처리가, 위험요인을 완화할 수 있는 안전장치, 보안조치 및 메커니즘이 부재한 상황에서, 개인의 권리와 자유에 관하여 높은 수준의 위험요소를 초래한다고 보여주거나, 정보처리자가 해당 위험요소는 가용할만한 기술과 이행의 비용 면에서 합리적인 수단으로 완화될 수 없다고 의견을 내는 경우, 관련 감독기구는 처리활동 시작 이전에 자문을 해주어야 한다. 이러한 높은 수준의 위험요소는 특정 유형의 개인정보처리와 처리의 범위 및 빈도수에 따라 촉발될 수 있으며 이는 개인의 권리와 자유를 방해하거나 손상을 초래할 수 있다. 해당 감독기관은 지정된 기간 안에 자문 요청에 응답해야 한다. 그러나 해당 기간 동안 감독기관이 자문요청에 응답하지 않아도, 처리방식의 금지 권한 등, 이 법에 규정된 감독기구의 업무와 권한에 따라 감독기관의 어떠한 개입에도 불이익이 미치지 않아야 한다. 이러한 자문의 과정의 일환으로, 문제가 되는 처리와 관련해 수행되는 개인정보보호 영향평가의 결과는, 특히 개인의 권리와 자유에 관한 위험요소를 완화하기 위해 예상되는 조치는, 감독기관에 제출될 수 있다.
(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) 수탁처리자는, 필요 시 또는 요청에 따라, 개인정보보호 영향평가의 수행에서 파생되거나 감독기관의 사전 자문에서 파생되는 의무를 준수하기 위해 정보처리자를 도와야 한다.
(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) 감독기관의 자문은 개인정보의 처리를 위해 제공되는 법적, 규제적 조치의 준비 과정에서 또한 이루어져야 하며, 이는 이 법에 맞는 의도된 처리를 준수하고 특히 정보주체에 관련된 위험요인을 완화하기 위함이다.
(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	(97) 처리가 공공기관에 의해 수행되는 경우, 법원 또는 독립적인 사법기관이 그들의 사법적 능력에 따라 행동하는 경우를 제외하고, 민간 부문의 경우, 처리가, 핵심활동이 정보주체에 대한 규칙적이고 시스템적인 대규모 감시를 요구하는 처리방식으로 이루어진 정보처리자에 의해 수행되는 경우, 또는 정보처리자 또는 수탁처리자의 핵심 활동이 대규모의 특정범주의 개인정보와 형사기소 및 범죄에 관련된 개인정보에 대한 처리로 이루어진 경우, 개인정보보호법과 관행에 대해 전문가적 지

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.	식을 보유한 개인은 이 법의 내부적 준수를 감시하기 위해 정보처리자 또는 수탁처리자를 도와야 한다. 민간 부문에서, 정보처리자의 핵심활동은 정보처리자의 주된 활동에 관련 있으며, 개인정보의 처리가 보조적인 경우의 활동과는 관련이 없다. 필요한 전문적 지식의 수준은 정보처리자 또는 수탁처리자가 수행하는 개인정보 처리방식이나 처리된 개인정보에 요구되는 보호에 따라 특히 결정될 수 있다. 이러한 개인정보보호 담당관은 정보처리자의 고용인인지 여부와는 관계없이 독립적으로 본인의 업무와 임무를 수행해야 한다.
(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) 정보처리자 또는 수탁처리자의 범위를 대표하는 협회나 다른 기구는 이 법에서 정한 제한 선에서 행동강령을 정하도록 권장되며, 이를 통해 이 법의 효과적인 적용을, 특정 분야에서 수행되는 처리의 구체적인 특성과 영세 및 중소기업의 구체적인 필요성을 고려하여, 촉진할 수 있다.
(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) 행동강령을 정할 때 또는 이러한 강령의 범위를 변경하거나 확대할 때, 정보처리자 또는 수탁처리자의 범위를 대표하는 협회 또는 다른 기구들은, 가능한 경우 정보주체를 포함한 관련 이해관계자와 상의해야하며, 이러한 자문에 대한 답변에 나타난 견해와 수령 받은 제출 자료를 참작해야한다.
(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) 이 법의 준수와 투명성을 강화하기 위해서, 인증 메커니즘, 개인정보보호 인장 및 마크의 수립이 권장되어야 하며, 이를 통해 정보주체는 관련 제품 및 서비스에 대한 개인정보보호의 수준을 빠르게 평가할 수 있다.
(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	(101) 이전이 필요하다. 개인정보의 국외이전의 증가로 인해 개인정보 보호와 관련한 새로운 과제 및 문제가 생겨났다. 그러나 개인정보가 유럽연합에서 제3국의 정보처리자, 수탁처리자나 기타 수령인 또는 국제기구로 이전될 때, 본 규정에 의해 유럽연합 역내에서 보장되는 개인의 보호수준이 침해되어서는 안 되며, 이는 제3국이나 국제기구에서 향후 동일한 제3국이나 국제기구 또는 기타 제3국이나 국제기구의 정보처리자와 수탁처리자에게 개인정보가 이전되는 경우에도 그러하다. 어떤 경우에서도 제3국과 국제기구로의 정보 이전은 본 규정을 철저히 준수하여서만 시행될 수 있다. 개인정보 이전은 본 규정의 나머지 조문에 따라, 정보처리자나 수탁처리자가 본 규정의 조문에서 제3국이나 국제기구로의 개인정보 이전과 관련해 규정된 조건들을 준수할 경우에 한해서 시행될 수 있다.

with this Regulation. A transfer could take place only if, subject to the other provisions of this Regulation, the conditions laid down in the provisions of this Regulation relating to the transfer of personal data to third countries or international organisations are complied with by the controller or processor.	
(102) This Regulation is without prejudice to international agreements concluded between the Union and third countries regulating the transfer of personal data including appropriate safeguards for the data subjects. Member States may conclude international agreements which involve the transfer of personal data to third countries or international organisations, as far as such agreements do not affect this Regulation or any other provisions of Union law and include an appropriate level of protection for the fundamental rights of the data subjects.	(102) 본 규정은 유럽연합과 제3국간에 정보주체를 위한 적절한 안전조치 등의 개인정보 이전과 관련하여 체결된 국제협약을 침해하지 않는다. 회원국들은 제3국 또는 국제기구로의 개인정보 이전에 관한 국제협약을 체결할 수 있다. 단, 그러한 국제협약이 본 규정서나 기타 유럽연합 법률의 조항에 영향을 미치지 않고 정보주체의 기본권에 대해 적정한 보호수준을 포함한 경우에 한해서 그러하다.
(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) 집행위원회는 제3국, 제3국의 영토나 지정 부문 또는 국제기구가 적절한 수준의 개인정보 보호를 제공한다는 유럽연합 전역에 효력을 가지는 결정을 내림으로써 적절한 보호수준을 제공한다고 간주되는 해당 제3국이나 국제기구에 대해 유럽연합 전역에 법적 확실성 및 획일성을 부여한다. 그 같은 경우, 해당 제3국이나 국제기구로의 개인정보 이전은 추가적인 인가를 받을 필요 없이 시행될 수 있다. 집행위원회는 해당 제3국이나 국제기구에 사유를 설명한 통지 및 성명서를 전달한 후, 이러한 결정을 철회할 수 있다.
(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) 인권보호 등 유럽연합 창설의 기반이 된 기본적 가치에 부합하여, 제3국 또는 제3국의 영토나 지정 부문의 평가 시 집행위원회는 해당 제3국이 법치주의, 국제인권 규범·기준 및 정의 구현, 그리고 공안·국방·국가안보 및 치안과 형법 등 자국의 전반적·분야별 법률을 준수하는지를 고려해야 한다. 제3국내의 영토나 지정 부문에 대한 적정성 결정의 채택에는 구체적인 정보처리 활동 및 유효하고 적용 가능한 법적 기준 및 법률의 영역 등 해당 국가의 명확하고 객관적인 기준이 고려되어야 한다. 해당 제3국은 유럽연합 내에서 보장되는 수준에 본질적으로 상응하는 적정 수준의 개인정보 보호를 보장해야 한다. 이는 특히 개인정보가 하나 이상의 지정 부문에서 처리될 경우 더욱 그러하다. 해당 제3국은 효과적이고 독립적인 개인정보보호 감독을 보장하고 회원국의 DPA와의 협력 메커니즘을 가능하게 해야 한다. 관련 정보주체는 실효성을 띤 행사 가능한 권리 및 효과적인 행정적·사법적 구제방안을 제공받아야 한다.

(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) 제3국이나 국제기구가 체결한 국제협약과 별개로, 집행위원회는 해당 제3국이나 국제기구가 특히 개인정보 보호와 관련한 다자간·지역적 제도 참여로 부여받은 의무 및 그 같은 의무의 이행을 고려해야 한다. 특히 1981년 1월 28일자 개인정보 자동처리 및 추가 규약에 대한 개인의 보호에 관한 유럽평의회 협약에 대한 제3국의 가입 여부를 고려해야 한다. 집행위원회는 제3국 또는 국제기구의 보호 수준을 평가할 시 각료이사회의 자문을 구해야 한다.

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

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

(106) 집행위원회는 제3국, 제3국내의 영토나 지정 부문, 또는 국제기구의 정보 보호수준에 대한 적정성 결정이 제대로 작동하는지 모니터링하고 지침 95/46/EC의 제25조(6) 또는 제26조(4)를 근거로 채택된 결정이 제대로 작동하는지 모니터링 해야 한다. 집행위원회는 적정성 결정이 제대로 작동하는지 정기적인 검토를 위한 메커니즘을 규정해야 한다. 정기적인 검토는 해당 제3국이나 국제기구와 협의하여 해당 제3국이나 국제기구 내의 모든 관련 추이를 참작하여 시행되어야 한다. 감시 및 정기적 검토 시행의 목적으로 집행위원회는 유럽의회와 각료이사회, 그리고 기타 관련 기구의 의견 및 조사결과를 참작해야 한다. 집행위원회는 적정한 시간 내에 후속적인 결정들의 작동을 평가하고 그 결과를 유럽의회·각료이사회 규정서 (EU) No 182/2011에 규정된 위원회(Committee), 유럽의회, 그리고 각료이사회에 보고해야 한다.

(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.

(107) 집행위원회는 제3국, 제3국내의 영토나 지정 부문, 또는 국제기구가 더 이상 적정한 수준의 개인정보보호를 보장하지 않는다고 인지할 수 있다. 따라서 의무적 기업 규칙 등 적절한 안전조치가 수반된 정보이전과 관련한 본 규정의 요건 및 특정 상황에서의 적용의 일부 제외가 충족되지 않는 한 해당 제3국이나 국제기구로의 개인정보 이전은 금지되어야 한다. 이 같은 경우, 집행위원회와 해당 제3국이나 국제기구 간의 협의에 대한 규정이 마련되어야 한다. 집행위원회는 시기적절하게 관련 제3국이나 국제기구에 사유를 통보하고 상황 해결을 위한 협의에 들어가야 한다.

(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) 적정성 결정이 없을 경우, 정보처리자나 수탁처리자는 정보주체를 위한 적절한 안전조치를 통해 제3국에서의 정보보호의 미흡함을 보완하기 위한 조치를 취해야 한다. 이 같은 적절한 안전조치로 의무적 기업규칙, 집행위원회가 채택한 정보보호표준조항, 감독기관이 채택한 정보보호표준조항 또는 감독기관이 승인한 계약 조항을 활용할 수 있다. 이 같은 안전조치는 유럽연합 역내나 제3국에서 개인정보 보호 요건 및 효과적인 행정적 또는 사법적 구제 획득 및 보상 청구 등의 구속력 있는 정보주체의 권리와 효과적인 법적 구제의 가용성 등 유럽연합 역내에서의 개인정보 처리에 상응하는 정보주체의 권리 준수를 보장해야 한다. 이 같은 안전조치는 특히 개인정보 처리에 관한 일반 원칙과 설계 및 기본설정에 의한 개인정보 보호 원칙의 준수와 관련이 있다. 정보이전은 공공기관이나 기구에 의해 제3국의 공공기관이나 기구 또는 상응하는 의무나 기능을 가진 국제기구와 함께 양해각서 등 행정 협정에 삽입될 규정을 근거로 하는 등 정보주체에게 구속력 있고 효과적인 권리를 제공하여 시행될 수 있다. 법적 구속력이 없는 행정 협정에 안전조치가 제시될 경우 관련 감독기관의 인가가 필요하다.
(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) 정보처리자나 수탁처리자가 집행위원회나 감독기관이 채택한 정보보호표준조항을 활용할 가능성이 정보처리자나 수탁처리자가 당해 수탁처리자와 기타 수탁처리자 간의 계약 등 보다 광범위한 계약에 정보보호표준조항을 포함시키는 것을 금지하거나, 만약 기타 조문이나 안전조치의 추가가 집행위원회나 감독기관이 채택한 표준계약조항에 직·간접적으로 위배되지 않고 정보주체의 기본권이나 자유를 침해하지 않는 경우 정보처리자나 수탁처리자에 의한 조항이나 안전조치의 추가를 금지해서는 아니 된다. 정보처리자와 수탁처리자는 정보보호표준조항을 보충하는 계약적 의무를 통해 추가적인 안전조치를 제공할 수 있어야 한다.
(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) 공동 경제활동에 종사하는 사업체나 기업 집단은 유럽연합으로부터 공동 경제활동에 종사하는 동일 사업체나 기업 집단 내 단체로의 개인정보 국외이전을 위해 승인된 의무적 기업규칙을 활용할 수 있어야 한다. 단, 그 같은 의무적 기업규칙에 개인정보 이전 또는 개인정보 이전의 범주에 대한 적정한 안전조치를 보장하는 모든 필수적인 원칙과 구속력 있는 권리가 포함되어야 한다.
(111) Provisions should be made for the possibility for transfers in	(111) 정보주체가 명백한 동의를 제공한 경우이거나 정보이전이 간헐적이고

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.

계약 또는 사법절차에 따른 것인지, 규제기구의 절차 등 행정적 또는 법원 이외의 다른 절차에 따른 것인지에 관계없이 법적 청구와 관련해 이전이 필요한 특정 상황에 대한 개인정보 이전의 가능성이 규정되어야 한다. 정보이전이 유럽연합 또는 회원국 법률이 규정한 중요한 공익의 근거로 요구되는 경우 또는 일반에 공개되거나 정당한 이익을 가진 사람들의 참조(조회)의 목적으로 법률에 의해 작성된 개인정보 기록부(register)로부터 시행되는 경우에 대한 정보이전의 가능성도 규정되어야 한다. 후자의 경우에 시행되는 정보이전에는 개인정보 기록부(register)에 포함된 개인정보의 전체 또는 정보의 전체 범주가 관련되어서는 안 된다. 그리고 개인정보 기록부(register)가 정당한 이익을 가진 사람의 참조용도일 때, 정보주체의 이익 및 기본권을 전적으로 고려하여, 정당한 이익을 가진 해당인의 요청에 한해서 또는 그들이 수령인이 될 경우에만 정보이전이 가능하다.

(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) 적용의 일부 제외는 특히 중요한 공익상의 이유로 요구되고 필요한 개인정보의 이전에 적용되어야 한다. 전자의 사례는 경쟁감독기관, 국세청 또는 관세청 간이나 금융 감독기관 간, 또는 사회보장 담당기관 간에 국제적인 정보교류가 이루어지는 경우이고 후자의 사례로는 전염병 접촉 경로 추적이나 스포츠 경기에서 도핑의 감소·근절을 위한 공공보건의 경우가 해당한다. 또한 정보주체가 동의를 제공할 수 없는 경우에는 정보주체나 제3자의 생명에 관한 이익을 위하여 필수적인 이익을 보호하는데 필요한 경우 개인정보의 이전은 적법한 것으로 간주되어야 한다. 적정성 결정이 없을 경우, 유럽연합 또는 회원국 법률은 중요한 공익상의 이유로 특정 범주의 개인정보를 제3국이나 국제기구에 이전하는 것을 명시적으로 제한할 수 있다. 회원국은 이에 해당하는 규정을 집행위원회에 고지해야 한다. 신체적 또는 법적으로 동의를 할 수 없는 정보주체의 개인정보를 제네바협정으로 부과된 업무를 수행하기 위하여 또는 무력분쟁에 적용 가능한 국제인도법을 준수하기 위해 인도적 성격의 국제기구로 이전하는 것은 중요한 공익상의 이유 또는 해당 정보주체의 생명에 관한 이익에 속하기 때문에 필요한 것으로 간주될 수 있다.

(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

(113) 정보주체의 이익이나 권리 및 자유가 컨트롤러가 추구하는 정당한 이익에 우선하지 않는 경우로서 컨트롤러가 개인정보 이전과 관련된 모든 정황을 평가했을 때, 간헐적이고 한정된 숫자의 정보주체에만 관련되는 정보이전이 컨트롤러가 설득력 있는 정당한 이익을 추구하는 목적으로 가능할 수도 있다. 컨트롤러는 개인정보의 성격, 예정된 정보처리 작업(들)의 목적 및 지속기간, 개인정보 발송국가, 제3국 및 정보가 최종 이전되는 국가의 상황, 본인의 개인정보 처리와 관련해 개인의 기본권 및 자유를 보호하는데 적절한 안전장치를 특히 고려해야 한다. 이 같은 정보이전은 정보이전을 위한 기타 근거가 적용 가능하지 않은 나머지 경우에서만 가능하다. 과학이나 역사적 연구의 목적 또는 통계의 목적으로, 지식의 증진이라는 사회의 합당한 기대 또한 고려되어야 한다. 컨트롤러는 정보이전에 대하여 감독기관 및

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.

해당 정보주체에 고지해야 한다.

(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) 어떤 경우에서도, 집행위원회가 제3국의 적정한 보호수준에 대해 아무런 결정을 내리지 않았을 경우, 정보처리자나 수탁처리자는 일단 개인정보가 이전된 후 정보주체에게 유럽연합 내에서 시행되는 본인의 개인정보처리에 대한 구속력 있고 효과적인 권리를 제시하는 해결방안을 통해 정보주체가 계속적으로 기본권 및 안전조치의 혜택을 받도록 해야 한다.

(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 inter alia be the case where the disclosure is necessary for an important ground of public interest recognised in Union or Member State law to which the controller is subject.

(115) 일부 제3국은 회원국 소관의 개인과 법인의 개인정보 처리 활동을 직접 규제하기 위한 취지의 법률, 규정 및 기타 입법 기구를 제정한다. 여기에는 정보처리자나 수탁처리자에게 개인정보의 이전이나 공개를 요구하는 제3국의 법원이나 재판소의 판결 또는 행정당국의 결정이 포함될 수 있다. 이 같은 판결이나 결정은 요청을 한 제3국과 유럽연합 또는 회원국 간에 시행 중인 사법공조조약 등의 국제협정에 기반을 두지 않는다. 이 같은 법률, 규정 및 기타 입법 기구의 역외 적용은 국제법에 위반될 수 있고 본 규정이 유럽연합 내에서 보장하는 개인에 대한 보호를 저해할 수 있다. 정보이전은 제3국으로의 정보이전을 위한 본 규정의 조건을 만족시키는 경우에 한해서만 허용되어야 한다. 정보처리자에 적용되는 유럽연합이나 회원국의 법률에 인지된 공익의 중요한 근거를 위해 정보공개가 필요한 경우가 특히 이에 해당한다.

(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

(116) 유럽연합 역외로의 개인정보 이전은 불법적인 개인정보 활용이나 공개로부터 스스로를 보호하고자 하는 등 개인이 개인정보 보호권을 행사하는 역량을 위태롭게 할 수 있다. 이와 동시에 감독기관은 역외 지역에서의 활동에 관해 민원을 처리하거나 조사를 시행할 수 없다고 생각할 수도 있다. 국가 간의 협력을 위한 노력은 불충분한 방지나 구제력, 모순된 법적제도 및 자원제약과 같은 실질적 장애물로 인해 저해될 수 있다. 따라서 정보교류 및 합동조사를 위해 개인정보보호 감독기구 간에 더욱 밀접한 협력을 증진시켜야 할 필요가 있다. 개인정보보호 법률 집행을 위한 국제상호지원을 용이하게 하는 국제협력 메커니즘의 개발을 목적으로, 집행위원회와 감독기구는 호혜를 바탕으로 본 규정을 준수하여 정보를 교환하고 권한 행사와 관련된 활동에 있어 제3국의 주무당국과 협력하여야 한다.

information and cooperate in activities related to the exercise of their powers with competent authorities in third countries, based on reciprocity and in accordance with this Regulation.	
(117) The establishment of supervisory authorities in Member States, empowered to perform their tasks and exercise their powers with complete independence, is an essential component of the protection of natural persons with regard to the processing of their personal data. Member States should be able to establish more than one supervisory authority, to reflect their constitutional, organisational and administrative structure.	(117) 완전한 독립성을 가지고 업무를 수행하고 권한을 행사할 수 있는 감독기관을 회원국에 설립하는 것은 개인의 개인정보 처리와 관련해 해당인을 보호하는데 필수적인 요소이다. 회원국은 헌법적, 조직적, 행정적 구조를 반영하여 하나 이상의 감독기관을 설립해야 한다.
(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) 감독기관의 독립성은 해당 감독기관이 재정지출이나 사법심사와 관련한 통제 또는 모니터링의 대상이 될 수 없다는 것을 의미하지 않는다.
(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) 회원국이 여러 개의 감독기관을 두는 경우, 해당 국가는 감독기관들이 본 규정의 일관적 적용을 위한 메커니즘에 효율적으로 참여할 수 있도록 하는 메커니즘을 법으로 정해야 한다. 해당 회원국은 특히 감독기관들이 그 같은 메커니즘에 효율적으로 참여할 수 있도록 단일 연락거점의 역할을 할 감독기관을 지정하여 기타 감독기관, 각료이사회 및 집행위원회와 원만한 협력을 할 수 있도록 해야 한다.
(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) 각 감독기관은 유럽연합 전역의 기타 감독기관들과의 상호지원 및 협력과 관련된 업무 등 효과적인 업무수행에 필요한 재정·인적자원, 부지, 기반시설을 제공받아야 한다. 각 감독기관은 연간 별도의 공공예산을 받아야 하는데 이 예상은 전체 국가 예산의 일부일 수 있다.
(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	(121) 각 회원국은 법률로써 감독기관의 단일 또는 복수의 위원에 대한 일반적 요건을 규정해야 하고 특히 그 위원들이 투명한 절차를 통해 임명되어야 한다고 규정해야 한다. 위원은 정부, 정부각료, 의회나 상원 또는 하원의 제안으로 회원국의 의회, 행정부 또는 정부수반에 의해 임명되거나 회원국 법률로 위임된 독립기구에 의해 임명된다. 감독기관의 독립성을 보장하기 위해, 감독기관의 구성원은 품위를 유지해야 하고 직무와 부합되지 않는 행동을 제한하며, 임기 중에 보수의 유무와 상관없이 양립 가능하지 않은 직업에 종사해서는 안 된다. 감독기관은 감독기관 또는 회원국 법률로 설립된 독립기구가 선발한 자체의 직원을 두어야 하고 이들은 전적으로 감독기관의 위원 또는 위원들의 지시를 따라야 한다.

exclusive direction of the member or members of the supervisory authority.	
(122) Each supervisory authority should be competent on the territory of its own Member State to exercise the powers and to perform the tasks conferred on it in accordance with this Regulation. This should cover in particular the 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) 각 감독기관은 자국의 영토에서 본 규정에 따라 부여받은 권한을 행사하고 업무를 수행할 수 있어야 한다. 특히 정보처리자나 수탁처리자가 자국 영토에 설립한 사업장의 활동 중의 정보처리, 공익의 행사를 위해 공공기관이나 민간기구가 시행하는 개인정보 처리, 자국 영토의 정보주체에 영향을 미치는 정보처리, 또는 유럽연합 역내에 설립되지 않는 정보처리자나 수탁처리자가 본인이 속한 국가에 거주하는 정보주체를 대상으로 시행하는 정보처리가 이에 해당한다. 정보주체가 제기한 민원처리, 본 규정서 적용에 대한 조사 실시, 개인정보 처리와 관련한 위험, 규칙, 안전조치 및 권리에 대한 공공의식의 향상이 이에 포함된다.
(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) 감독기관은 본 규정에 따른 조문의 적용을 모니터링하고 유럽연합 전역에 일관적인 적용이 되도록 함으로써 개인정보 처리와 관련한 개인을 보호하고 역내시장 내에서 개인정보의 자유로운 이동을 용이하게 해야 한다. 그 같은 목적으로 감독기관은 상호지원 제공이나 협력에 대해 회원국 간에 협정을 맺을 필요 없이 상호 간에, 그리고 집행위원회와 협력해야 한다.
(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) 유럽연합 역내의 정보처리자나 수탁처리자의 한 사업장의 활동 중 개인정보 처리가 이루어지고 정보처리자나 수탁처리자가 하나 이상의 회원국에 배치된 경우, 또는 유럽연합 역내에 설립된 정보처리자나 수탁처리자의 단일 사업장의 활동 중에 시행되는 정보처리가 하나 이상의 회원국의 정보주체에 실질적으로 영향을 미치거나 실질적인 영향을 미칠 가능성이 있는 경우, 해당 정보처리자나 수탁처리자의 주 사업장 또는 단일 사업장을 관할하는 감독기관이 선임 감독기관이 된다. 선임 감독기관은 모든 관련 기관과 협력해야 한다, 그 이유는 관련 정보처리자나 수탁처리자가 그 기관들의 국가의 영토에 사업장을 두었거나, 그 기관들의 국가의 영토에 거주하는 정보주체가 실질적인 영향을 받았거나, 또는 그 기관들에 민원이 제기되었기 때문이다. 해당 회원국에 거주하지 않는 정보주체가 민원을 제기한 경우, 민원을 제소 받은 감독기관도 선임 감독기관이 되어야 한다. 각 료이사회는 본 규정의 적용에 관한 질의사항에 대해 가이드라인을 발행하는 업무 중에서 질의대상이 된 개인정보의 처리가 하나 이상의 회원국 내의 정보주체에게 실질적인 영향을 끼쳤는지 확인하기 위해 고려해야 할 기준 및 유관하고 합리적인 이의를 구성하는 요소에 대한 기준 등에 관한 가이드라인을 제정할 수 있어야 한다.

(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) 선임 감독기관은 본 규정에 따라 부여받은 권한을 적용하는 조치에 대한 법적 구속력이 있는 결정을 채택할 수 있어야 한다. 선임 감독기관으로서의 역량을 발휘해 의사결정 과정에 관련 감독기관들을 밀접히 관여시키고 조정해야 한다. 정보주체가 제기한 민원을 전부 또는 부분적으로 거부하는 결정을 내리는 경우 그 결정은 민원이 제기된 감독기관이 채택하여야 한다.
(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) 결정은 선임 감독기관 및 관련 감독기관들에 의해 공동으로 합의되어야 하고, 정보처리자나 수탁처리자의 주 사업장이나 단일 사업장을 대상으로 하며, 정보처리자와 수탁처리자에 대해 구속력이 있어야 한다. 정보처리자나 수탁처리자는 본 규정의 준수 및 선임 감독기관이 유럽연합 내 개인정보 처리활동에 대해 정보처리자나 수탁처리자의 주 사업장에 통보한 결정의 이행을 보장하기 위해 필요한 조치를 취해야 한다.
(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 authorites 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) 선임 감독기관의 역할을 하지 않는 각 감독기관은 정보처리자나 수탁처리자가 하나 이상의 회원국에 설립된 경우 해당 지역의 사안을 처리할 수 있어야 한다. 그러나 특정 정보처리의 대상은 단일 회원국 내에서 시행되는 처리에만 관여되고 해당 단일 회원국 내의 정보주체만을 관련시켜야 한다. 예를 들어, 정보처리가 한 회원국 내의 특정 고용분야의 피고용인들의 개인정보 처리에 관한 경우, 감독기관은 선임 감독기관에 그 사안에 대해 지체 없이 통보해야 한다. 선임 감독기관은 통보를 받은 후 선임 감독기관과 기타 관련 기관들 사이의 협력에 대한 조문(one-stop-shop 메커니즘)에 따라 해당 사안을 처리할 것인지 여부 또는 통보를 해온 감독기관이 지역 차원에서 해당 사안을 처리할 것인지 여부를 결정해야 한다. 자체적으로 해당 사안을 처리할 것인지 여부를 결정할 때, 선임 감독기관은 정보처리자나 수탁처리자에 관한 결정의 효과적인 이행을 보장하기 위해 통보를 해온 감독기관이 속한 회원국 내에 소재한 정보처리자나 수탁처리자의 사업체가 있는지 여부를 고려해야 한다. 선임 감독기관이 해당 사안을 처리하기로 결정하는 경우, 그것에 대해 통보를 한 감독기관은 결정에 대한 초안을 제출할 여지를 가져야 하고 그 초안은 선임 감독기관이 one-stop-shop 메커니즘의 틀 안에서 결정(안)을 준비할 때 최대한으로 고려해야 하는 것이다.
(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	(128) 선임 감독기관 및 one-stop-shop 메커니즘에 대한 규정은 공공기관이나 민간기구가 공익을 위해 정보처리를 시행하는 경우에는 적용되어서는 아니 된다. 그 같은 경우 본 규정에 따라 부여받은 권한을 행사할 수 있는 감독기관만이 해당 공공기관이나 민간기구가 설립된 회원국의 감독기관이 되어야 한다.

conferred to it in accordance with this Regulation should be the supervisory authority of the Member State where the public authority or private body is established.

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

(129) 유럽연합 전역에서의 본 규정의 일관성 있는 모니터링 및 집행을 보장하기 위해, 감독기관들은 각 회원국 내에서 동일한 업무 및 조사권, 시정권·제재 및 승인·자문 권한 등의 동일한 권한을 가져야 하고 이는 특히 개인이 제기한 민원의 경우 더욱 그러하며, 회원국 법률에 따른 기소(검찰) 기관이 본 규정의 위반을 사법 기관에 제소하고 소송 절차에 관여할 권한을 침해해서는 아니 된다. 이 같은 권한에는 금지 등 정보처리를 임시적으로 또는 완전히 제한하는 권한도 포함된다. 회원국들은 본 규정에 의해 개인정보 보호와 관련된 기타 업무를 규정할 수 있다. 감독기관의 권한은 유럽연합 또는 회원국 법률에 제시된 적절한 절차의 안전조치에 따라 공정하고 적정한 시간 내에 행사되어야 한다. 특히 각 조치는 개별 사안의 정황을 참작하여 본 규정의 준수를 보장함에 있어 적절하고 필요한 것이어야 하고 개인에게 악영향을 끼칠 개별적 조치의 이행 전에 개개인의 발언할 권리를 존중하고 관계자에게 불필요한 비용 및 과도한 불편을 끼치는 것을 방지해야 한다. 부지(premises) 접근과 관련한 조사권한은 사전의 사법적 인가 등 회원국 절차법의 특정 요건에 부합하여 행사되어야 한다. 감독기관의 법적 구속력 있는 각각의 조치는 서면 형식으로 명료하고 명확해야 하고 조치를 발부한 감독기관, 조치 발부일, 기관장의 서명 또는 기관장이 인가한 감독기관 구성원의 서명을 포함하며 조치의 사유를 설명하고 유효한 구제 권리에 대해 명시하여야 한다. 이것이 회원국의 절차법에 따른 추가 요건을 배제해서는 아니 된다. 법적 구속력 있는 결정의 채택은 그 결정을 채택한 감독기관의 회원국에서 사법 심리가 발생할 수 있음을 내포한다.

(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) 민원이 제기된 감독기관이 선임 감독기관이 아닌 경우, 선임 감독기관은 본 규정의 협력 및 일관성에 대한 조문에 따라 해당 민원이 제기된 감독기관과 긴밀히 협력해야 한다. 이 같은 경우, 선임 감독기관은 행정 과태료 부과 등 법적 효력을 발생시킬 목적의 조치를 취할 때, 민원이 제기되고 관련 감독기관과의 협력 하에 자국의 영토에서 조사를 시행할 수 있는 감독기구의 견해를 최대한으로 고려해야 한다.

(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) 제3의 감독기관이 정보처리자나 수탁처리자의 정보처리 활동에 대한 선임 감독기관의 역할을 해야 하나 민원의 구체적인 사안이나 발생 가능한 침해행위가 민원이 제기되거나 발생 가능한 침해행위가 감지된 회원국 내의 정보처리자나 수탁처리자의 정보처리 활동에만 관여하고 그 사안이 기타 회원국의 정보주체에게 실질적인 영향을 미치거나 미칠 가능성이 없는 경우, 민원이 제기되거나 본 규정에 대해 가능한 침해행위가 수반되는 상황을 감지하거나 기타의 방식으로 통지받은 감독기관은 정보처리자와 원만한 해결방안을 모색해야 하고 이것이 성공적이지 못할 경우, 전범위의 권한을 행사해야 한다. 여기에는 감독기관의 회원국의 영토에서 시행되거나 그 회원국 영토의 정보주체에 관해 시행되는 특정한 개인정보 처리, 감독기구의 회원국 영토 내의 정보주체를 특정 대상으로 하여 재화 또는 서비스를 제공하는 상황에서 시행되는 개인정보 처리, 또는 회원국 법률에 따라 관련 법적 의무를 고려하여 평가되어야 하는 개인정보 처리가 포함되어야 한다.
(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) 일반을 대상으로 한 감독기관의 인식제고 활동에는 교육 분야의 개인과 영세기업·중소기업 등의 정보처리자와 수탁처리자에 초점을 맞춘 특정 조치들이 포함되어야 한다.
(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) 감독기관들은 역내시장에서의 본 규정의 일관된 적용과 시행을 보장하기 위해 업무 수행 시 서로 조력하고 상호지원을 제공해야 한다. 상호지원을 요청하는 감독기관은 상대 기관이 요청을 접수한 후 한 달 이내에 요청에 대한 답변을 받지 못하는 경우 임시조치를 채택할 수 있다.
(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) 각 감독기관은 적절한 경우 다른 감독기관들과의 공동 작업에 참여해야 한다. 요청을 받은 감독기관은 특정 기한 내에 요청에 응답할 의무가 있다.
(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	(135) 유럽연합 전체에 본 규정의 일관된 적용을 보장하기 위해, 감독기관들 사이에 협력을 위한 일관성 메커니즘이 제정되어야 한다. 이 메커니즘은 특히 감독기관이 여러 회원국의 다수의 정보주체에게 실질적인 영향을 미치는 정보처리 작업에 대해 법적 효력을 발생시킬 목적의 조치를 채택하려는 경우 적용되어야 한다. 이 메커니즘은 관련 감독기구나 집행위원회가 일관성 메커니즘에서 처리되어야 한다고 요청하는 사안에도 적용되어야 한다. 이 메커니즘은 집행위원회가 협약(Treaties)에 따라 권한을 행사하여 이행할 수 있는 조치를 침해해서는 아니 된다.

without prejudice to any measures that the Commission may take in the exercise of its powers under the Treaties.	
(136) In applying the consistency mechanism, the Board should, within a determined period of time, issue an opinion, if a majority of its members so decides or if so requested by any supervisory authority concerned or the Commission. The Board should also be empowered to adopt legally binding decisions where there are disputes between supervisory authorities. For that purpose, it should issue, in principle with a two-third 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) 일관성 메커니즘을 적용할 때, 유럽정보보호위원회(Board)는 구성위원의 과반수가 결정하거나 관련 감독기구나 집행위원회가 요청하는 경우, 정해진 기간 내에 의견서를 발표해야 한다. 또한 감독기관들 간에 분쟁이 있을 경우 법적 구속력이 있는 결정을 채택할 권한을 부여받아야 한다. 그 같은 목적으로, 유럽정보보호위원회는 협력 메커니즘 내에서 특히 본 규정의 침해 여부 등에 관해 선임 감독기관과 유관 감독기관들 간에 사안의 시비를 가리는 경우 등 감독기관들 간에 의견이 충돌할 때 원칙적으로 구성위원의 2/3의 찬성으로 명백하게 명시된 경우에 대해 법적 구속력 있는 결정을 발표해야 한다.
(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) 특히 정보주체의 권리 시행이 현저히 저해될 수 있는 위험이 존재할 때 정보주체의 권리와 자유를 보호하기 위한 조치가 시급히 요구될 수 있다. 따라서 감독기관은 자국 영토에서 3개월을 초과하지 않는 유효기간을 명시하여 적절히 타당한 임시적 조치를 채택할 수 있어야 한다.
(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) 그 같은 메커니즘의 적용은 적용이 의무적인 경우 감독기관이 취하는 법적 효력을 발생시킬 목적의 조치의 적법성을 위한 하나의 조건이 된다. 회원국 간에 관련이 있는 기타의 경우, 선임 감독기관과 유관 감독기관들 간에 협력 메커니즘이 적용되어야 하며 관련 감독기관들 간에 일관성 메커니즘의 작동 없이 양자간 또는 다자간의 기반으로 상호지원 및 공동 작업이 시행될 수 있다.
(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) 본 규정의 일관된 적용을 도모하기 위해, 유럽정보보호이사회가 유럽연합의 독립기구로 설립되어야 한다. 목표 달성을 위해 유럽정보보호이사회는 법인격을 가져야 하고 의장이 유럽정보보호이사회를 대표해야 한다. 유럽정보보호이사회는 지침 95/46/EC이 제정한 개인정보처리에 관한 개인보호 작업반을 대체해야 하고 각 회원국 감독기관의 장, 유럽개인정보보호기구(European Data Protection Supervisor) 또는 그에 상응하는 대표자로 구성되어야 한다. 집행위원회는 의결권 없이 유럽정보보호이사회의 활동에 참여하고 유럽개인정보보호기구는 특정 의결권을 보유해야 한다. 유럽정보보호이사회는 특히 제3국이나 국제기구의 보호 수준에 관하여 등 집행위원회에 자문을 제공하고 유럽연합 전역의 감독기관들의 협력을 도모함으로써 유럽연합 전역에 본 규정의 일관된 적용을 도와야 한다. 유럽정보보호이사회는 업무 수행 시 독립적으로 행동해야 한다.

(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) 유럽정보보호이사회는 유럽개인정보보호담당기구(European Data Protection Supervisor)가 제공하는 사무처의 지원을 받아야 한다. 본 규정에 의해 유럽정보보호이사회에 부관된 업무를 수행하는 유럽개인정보보호담당기구의 직원들은 오로지 유럽정보보호이사회 의장의 지시에 따라 업무를 수행하고 의장에게 보고해야 한다.
(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) 모든 정보주체는 특히 거주 회원국의 단일 감독기구에 민원을 제기할 권리 및 본 규정에 따른 본인의 권리가 침해된다고 생각하거나 정보주체의 권리보호를 위해 조치가 필요할 때에도 감독기관이 민원에 대해 조치를 취하지 않거나 부분적으로 또는 전적으로 민원을 거부하거나 묵살하는 경우 헌장 제47조에 따라 유효한 사법적 구제를 받을 권리를 가져야 한다. 민원에 따른 조사는 특정 경우에 적정선까지 사법 심리의 적용을 받아 실시되어야 한다. 감독기관은 적정 기간 내에 민원의 절차 및 결과에 대해 정보주체에 통지해야 한다. 해당 사안이 추가 조사나 다른 감독기관과의 협력을 요구하는 경우, 정보주체는 중간 정보를 제공받아야 한다. 민원 제출을 용이하게 하기 위해, 각 감독기관은 기타 통신 수단을 배제하지 않고 전자적으로도 작성이 가능한 민원 제출 양식을 제공하는 등의 조치를 취해야 한다.
(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) 정보주체가 본 규정에 따른 본인의 권리가 침해된다고 생각하는 경우, 해당인은 회원국 법률에 따라 설립되고 공익을 위한 법적 의무가 있으며 개인정보 보호 분야에 활동 중인 비영리 기구, 단체 또는 협회에게 본인을 대신하여 감독기구에 민원을 제기하고, 본인을 대신하여 사법적 구제를 받을 권리를 행사하고, 회원국 법률에 규정된 경우 본인을 대신해 보상을 받을 권리를 행사하도록 권한을 부여하는 권리를 가져야 한다. 회원국은 그 같은 기구, 단체나 협회가 정보주체의 권한과 상관없이 자국 내에서 민원을 제기할 권리 및 정보주체의 권리가 본 규정을 침해하는 개인정보 처리의 결과로 침해되었다고 간주할 사유가 있는 경우 유효한 사법적 구제를 받을 권리를 가지도록 규정할 수 있다. 해당 기구, 단체나 협회는 정보주체의 권한과 상관없이 정보주체를 대신하여 보상을 청구하지 못할 수도 있다.
(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	(143) 어떠한 개인 또는 법인이라도 유럽연합 기능에 관한 조약(TFEU) 제263조에 규정된 조건에 따라 유럽정보보호이사회의 결정을 취소하기 위해 사법재판소에 소송을 제기할 권리를 가진다. 그 같은 결정의 수신대상으로서, 결정에 대해 이의를 제기하고자 하는 관련 감독기관들

authorities concernedwhich 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 by Article 263 TFEU.

은 유럽연합 기능에 관한 조약(TFEU) 제263조에 따라 통지받은 후 두 달 이내에 소송을 제기하여야 한다. 유럽정보보호이사회의 결정이 정보처리자, 수탁처리자나 민원인에게 직간접적인 사안이 되는 경우, 후자는 유럽연합 기능에 관한 조약(TFEU) 제263조에 따라 유럽정보보호이사회의 홈페이지에 게시된 후 두 달 이내에 그 결정의 취소에 대한 소송을 제기할 수 있다. 유럽연합 기능에 관한 조약(TFEU) 제263조에 따른 이 권리를 침해하지 않고, 각 개인이나 법인은 본인에 대해 법적 효력을 발생시킬 감독기관의 결정에 대해 관할국의 법정에서 유효한 사법적 구제를 받아야 한다. 그 같은 결정은 특히 감독기관의 조사, 시정 및 인가 권한의 행사 또는 민원의 기각이나 거부와 관련된다. 그러나 유효한 사법적 구제에 대한 권리에는 감독기관이 발표한 의견이나 제공한 자문 등 법적 구속력이 없는 감독기관의 조치는 포함되지 않는다. 감독기관에 대한 소송 절차는 해당 감독기관이 설립된 회원국의 법정에서 해당 회원국의 절차법에 따라 시행되어야 한다. 해당 법정은 전적인 사법권을 행사해야 하고 여기에는 제기된 논쟁과 관련한 사실 및 법률에 대한 모든 질의사항을 검토하는 사법권도 포함되어야 한다. 감독기관이 민원을 거부하거나 기각한 경우, 해당 민원인은 동일한 회원국의 법정에 소송을 제기할 수 있다. 본 규정의 적용에 대한 사법적 구제의 경우, 문제시 되는 결정이 판결을 내리는데 필요하다고 간주하는 국가 법정들은 아마도, 또는 유럽연합 기능에 관한 조약(TFEU) 제267조에 규정된 경우에는 반드시, 사법재판소에 본 규정을 포함한 유럽연합 법률의 해석에 대한 선결적 판결을 요청해야 한다.

뿐만 아니라, 유럽정보보호이사회의 결정을 이행하는 감독기관의 결정에 대해 국가 법정에 소가 제기되고 위원회의 결정의 타당성(유효성)이 문제가 되는 경우, 해당 국가의 법정은 위원회의 결정이 무효하다고 판결 내릴 권한은 없지만 그 결정이 무효하다고 간주되는 경우, 유럽연합 기능에 관한 조약(TFEU) 제267조에 따라 타당성의 문제를 사법재판소에 회부하여 사법재판소가 해석하도록 해야 한다. 그러나 회원국의 법정은, 특히 해당 결정에 대해 직간접적으로 고심했던 경우, 해당 결정의 취소를 위한 소를 제기할 기회가 있었으나 유럽연합 기능에 관한 조약(TFEU) 제263조가 규정한 기간 내에 그렇게 하지 못한 개인이나 법인의 요청이 있을 시 유럽정보보호이사회의 결정의 타당성에 대한 문제를 회부하지 않을 수 있다.

(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,

(144) 감독기관의 결정에 대한 소송 절차를 관장하는 법정은 동일한 정보처리자나 수탁처리자에 의한 정보처리와 관련 있는 동일의 사안 등 동일한 개인정보 처리나 소송 사유에 관한 소송 절차에 대해 기타 회원국의 관련 법정에 소가 제기된다고 간주할 사유가 있다면, 그 같은 관련 소송 절차의 여부를 확인하기 위해 해당 법정에 연락을 취해야 한다. 관련 소송 절차가 기타 회원국의 법정에서 계류 중인 경우, 처음 소송 절차를 관장했던 법정 외에 모든 법정은 소송을 중지하거나, 당사자 한 측의 요청에 따라, 처음 소송 절차를 관장한 법정이 해당 소송 절차에 대한 사법권을 가지고 있고 그 국가의 법률이 관련 소송 절차의 통합을 허용하는 경우 해당 법정을 위해 사법권을

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.

거절할 수 있다. 소송 절차들은 매우 밀접히 연결되어 개별적인 소송 절차로 야기되는 양립 가능하지 않은 판결의 위험을 방지하기 위해 함께 심리하고 결정하는 것이 편리한 경우 서로 관련이 있다고 간주된다.

(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) 정보처리자나 수탁처리자에 대한 소송 절차에서 원고는 해당 정보처리자가 공적 권한을 행사하는 회원국의 공공기관이 아니라면 해당 정보처리자나 수탁처리자가 사업장을 가지고 있거나 관련 정보주체가 거주하는 회원국의 법정에 소를 제기할 선택의 여지가 있어야 한다.

(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) 정보처리자나 수탁처리자는 본 규정을 침해한 개인정보 처리의 결과로 개인이 감내해야 할지 모르는 피해 일체를 보상해야 한다. 정보처리자나 수탁처리자는 해당 피해에 대해 어떠한 방식으로도 책임이 없음을 입증하는 경우 책임을 면제받아야 한다. 피해의 개념은 사법재판소의 판례법을 고려하여 본 규정의 목적을 전적으로 반영하는 방식으로 광범위하게 해석되어야 한다. 이는 유럽연합 또는 회원국 법률의 기타 규정의 위반으로 야기된 피해에 대한 배상 청구를 침해하지 않는다. 본 규정을 침해하는 개인정보 처리에는 본 규정서 및 본 규정서의 규정을 명시한 회원국 법률에 따라 채택된 위임·시행법률을 침해하는 개인정보 처리도 포함된다. 정보주체는 본인이 겪은 피해에 대해 전액의 실질적인 보상을 받아야 한다. 정보처리자나 수탁처리자가 동일한 정보처리에 연루된 경우, 각 정보처리자나 수탁처리자는 전체 피해에 대해 책임을 져야 한다. 그러나 그들이 동일한 소송 절차에 연결된 경우로서 피해를 입은 정보주체에게 전액의 실질적인 보상이 보장된다면, 회원국 법률에 의거하여, 해당 정보처리로 야기된 피해에 대한 각 정보처리자나 수탁처리자의 책임에 따라 보상이 배분될 수 있다. 전액 보상을 지급한 정보처리자나 수탁처리자는 차후 동일한 정보처리 건에 관련된 기타 정보처리자나 수탁처리자들에 대해 상소 절차를 개시할 수 있다.

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

(147) 본 규정에 특히 정보처리자나 수탁처리자로부터 보상 등의 사법적 구제를 구하는 절차에 관하여 등 사법권에 대한 특정 규정이 포함된 경우, 유럽의회 및 각료이사회 규정서 (EU) No 1215/2012의 규정 등 일반적인 사법권의 규정이 그 같은 특정 규정의 적용을 침해해서는 아니 된다.

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

(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 appropriateprocedural safeguards in accordance with the general principles of Union law and the Charter, including effective judicial protection and due process.

(148) 본 규정서의 규정의 시행을 강화하기 위해, 본 규정에 따라 감독기관이 취한 적절한 조치에 더하거나 이를 대신하여 본 규정의 침해에 대해 행정 과태료 등 처벌이 부과되어야 한다. 경미한 침해의 경우나 부과될 것으로 예상되는 과태료가 개인에게 불균형한 부담이 되는 경우, 과태료 대신 징계를 내릴 수 있다. 그러나 침해의 성격, 중대성 및 지속기간, 침해의 의도적인 특징, 피해 완화를 위해 취한 조치, 책임의 정도나 관련 침해행위의 전례 여부, 침해 사실이 감독기관에 통지된 방식, 정보처리자나 수탁처리자에게 명한 조치의 준수, 행동강령 준수 및 기타 악화 또는 완화의 요인을 특히 고려해야 한다. 행정 과태료 등 벌금의 부과는 유효한 사법적 보호 및 정당한 법 절차 등 유럽연합 법률 및 헌장의 일반 원칙에 부합하는 적정한 절차적 안전조치에 따른 것이어야 한다.

(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) 회원국들은 본 규정에 따라 본 규정의 한도 내에서 채택된 국가 규정의 침해에 대하여 등 본 규정의 침해에 대한 형사처벌을 규정할 수 있어야 한다. 그 같은 형사처벌에는 본 규정의 침해를 통해 얻은 이익의 박탈도 고려되어야 한다. 그러나 그 같은 국가 규정의 침해에 대한 형사처벌 및 행정 과태료의 부과가 사법재판소가 해석한 일사부재리의 원칙의 침해로 이어져서는 아니 된다.

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

(150) 본 규정의 침해에 대한 행정 과태료를 강화하고 통일시키기 위해, 각 감독기관은 행정 과태료를 부과할 권한을 가져야 한다. 본 규정은 침해행위 및 관련 행정 과태료를 정하기 위한 상한선과 기준을 명시해야 한다. 관련 행정 과태료를 정하기 위한 상한선 및 기준은 각 개별 건에서 해당 감독기관이 특정 상황에 대한 모든 관련 정황을 고려하여 결정해야 하고, 특히 침해 및 침해결과의 성격, 중대성과 지속기간, 그리고 본 규정에 따른 의무의 준수를 보장하고 침해의 결과를 방지하거나 완화하기 위한 조치를 고려해야 한다. 행정 과태료가 한 사업체에 부과되는 경우, 사업체는 그 같은 목적으로 유럽연합 기능에 관한 조약(TFEU) 제101 및 102조에 따른 사업체로 이해되어야 한다. 행정 과태료가 사업체가 아닌 개인에 부과될 경우, 감독기관은 과태료의 적정 금액을 고려할 시 해당인의 경제적 여건과 회원국의 전반적 소득 수준을 참작해야 한다. 행정 과태료의 일관된 적용을 도모하는데 일관성 메커니즘이 활용될 수도 있다. 공공기관이 행정 과태료의 적용을 받는지 여부 및 그 정도는 회원국이 결정해야 한다. 행정 과태료를 부과하거나 경고장을 발부하는 것은 감독기관이 가진 기타 권한 또는 본 규정에 따른 기타 처벌의 적용에 영향을 미치지 않는다.

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.	
(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 misdemeanor 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) 덴마크와 에스토니아의 법제도는 본 규정서가 정한 행정 과태료를 고려하지 않는다. 행정 과태료에 대한 규정은 덴마크에서는 관할국의 법정이 형사처벌로서 과태료를 부과하고 에스토니아에서는 경범죄의 프레임워크 내에서 감독기관이 과태료를 부과하는 방식으로 적용될 수 있다. 단, 상기 회원국에서의 그 같은 규정의 적용이 감독기관이 부과하는 행정 과태료에 상응하는 효력을 지닐 경우에 그러하다. 따라서 관할국의 법정은 과태료를 부과한 감독기관의 제안을 고려하여야 한다. 어떠한 경우에서도, 부과된 과태료는 유효하고 온당하며 (침해행위를 하지 않도록 하는) 억지력이 있어야 한다.
(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) 본 규정에서 행정적 처벌이 통일되어 있지 않거나 본 규정의 중대한 침해의 경우 등 기타의 경우에서 필요한 경우, 회원국들은 유효하고 온당하며 (침해행위를 하지 않도록 하는) 억지력이 있는 처벌을 규정하는 제도를 시행해야 한다. 그 같은 처벌의 성격이 형사적 또는 행정적인지는 회원국 법률에 의해 결정되어야 한다.
(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) 회원국 법률은 언론, 학술, 예술 및 문학적 표현 등 표현과 정보의 자유를 통제하는 규정과 본 규정에 따른 개인정보 보호권 사이의 균형을 유지시켜야 한다. 단지 언론 목적이나 학술, 예술 또는 문학적 표현의 목적을 위한 개인정보 처리는 유럽연합 헌장 제11조에 구현된 바와 같이 개인정보 보호권과 표현 및 정보의 자유권 사이에 균형을 유지시킬 필요가 있을 경우, 본 규정의 특정 조문의 일부 제외 또는 면제를 따른다. 이는 특히 시청각 분야 및 뉴스 아카이브와 언론 도서관에서 개인정보를 처리할 때 적용된다. 따라서 회원국은 이 같은 기본권 간의 균형을 유지시키려는 목적에 필요한 적용의 면제 및 일부 제외를 규정하는 입법적 조치를 채택해야 한다. 회원국은 통칙(general principles), 정보주체의 권리, 정보처리자와 수탁처리자, 협력 및 일관성, 그리고 특정 정보처리 상황에 대해 이 같은 적용의 면제 및 일부 제외를 채택해야 한다. 회원국 간에 이 같은 면제 또는 일부 제외가 상이한 경우, 정보처리자가 따라야 하는 회원국의 법률이 적용되어야 한다. 모든 민주사회에서 표현의 자유권이 가지는 중요성을 고려하기 위해 저널리즘(journalism) 등의 자유에 관계되는 개념을 광범위하게 해석할 필요가 있다.

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

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

(154) 본 규정은 본 규정의 적용 시 공문서 공개열람의 원칙이 고려되도록 한다. 공문서의 공개열람은 공익을 위한 것으로 간주될 수 있다. 공공기관이나 공공기구가 보유한 문서상의 개인정보는 해당 기관이나 기구가 적용을 받는 유럽연합 또는 회원국 법률이 공개를 규정하고 있을 경우 그 기관이나 기구에 의해 공개될 수 있어야 한다. 그 같은 법률은 공문서의 공개열람 및 공공부문 정보의 재활용과 개인정보 보호권 간의 균형을 유지시켜야 하고 따라서 본 규정에 의거하여 요구되는 개인정보 보호권과의 균형 유지에 대해 규정할 수 있다. 이 같은 공공기관 및 기구에는 문서 공개열람에 대해 회원국의 법률이 다루는 모든 기관이나 기구가 포함된다. 유럽의회 및 각료이사회 지침 2003/98/EC은 유럽연합 및 회원국의 법조문에 따른 개인정보 처리와 관련한 개인의 보호 수준에 손을 대지 않고 어떠한 방식으로도 영향을 미치지 않으며 특히 본 규정에 규정된 의무 및 권리를 변경하지 않는다. 특히 그 지침은 개인정보 보호를 근거로 열람 제도(access regime)에 의해 열람이 배제되거나 제한되는 문서 및 그 같은 열람 제도를 통해 열람은 가능하나 그 재활용이 개인정보 처리에 관한 개인의 보호에 대한 법률과 양립하지 않는다고 법률로써 규정된 개인정보를 포함하는 문서의 일부에는 적용되지 않는다.

(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) 회원국 법률 또는 '업무 협정서' 등 단체 협약은 고용 환경에서 피고용인의 개인정보의 처리에 대해 특정 규정을 규정할 수 있고, 특히 고용 환경에서 개인정보가 피고용인의 동의, 고용 목적, 법률이나 단체 협약이 규정한 채무이행 등 고용 계약의 이행, 작업의 관리·계획·조직, 직장 내의 평등·다양성, 작업 중의 건강·안전을 근거로 처리되고, 개별 또는 단체적 차원에서 고용과 관련한 권리 및 혜택을 행사하기 위한 목적으로 처리되며, 고용 관계의 종결을 목적으로 처리되는 조건에 대해 규정할 수 있다.

(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

(156) 공익을 위한 유지보존의 목적, 과학이나 역사적 연구의 목적 또는 통계 목적에서의 개인정보 처리는 본 규정에 따른 정보주체의 권리와 자유를 위해 적절한 안전조치의 적용을 받아야 한다. 그 같은 안전조치를 통해 특히 데이터 최소화의 원칙을 보장하기 위한 기술·관리적 조치가 구비되어 있어야 한다. 공익을 위한 유지보존의 목적, 과학이나 역사적 연구의 목적 또는 통계 목적에서의 추가적인 개인정보 처리는 개인정보의 가명처리 등 적절한 안전조치가 존재하는 경우로서 정보처리자가 정보주체를 식별할 수 없거나 더 이상 식별할 수 없는 개인정보를 처리하여 그 같은 목적을 충족시킬 가능성을 평가하였을

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.

때 시행되어야 한다. 회원국은 공익을 위한 유지보존의 목적, 과학이나 역사적 연구의 목적 또는 통계 목적에서의 개인정보 처리를 위한 적절한 안전조치를 규정하여야 한다. 회원국은 특정 조건 하에서 정보주체를 위한 적절한 안전조치에 따라, 정보의 요건에 관하고 공익을 위한 유지보존의 목적, 과학이나 역사적 연구의 목적 또는 통계 목적으로 개인정보를 처리할 때 수정·삭제할 권리, 잊힐 권리, 정보를 이전하고 반대할 권리에 관하여 세부사항 및 적용의 일부 제외를 규정할 권한이 있어야 한다. 그 같은 조건과 안전조치에는 정보주체가 상기 권리를 행사하는 것에 대한 특정 절차가 포함될 수 있다. 단, 이것이 비례성 및 필요성의 원칙에 따라 개인정보 처리를 최소화하려는 목적의 기술·관리적 조치와 함께 특정 개인정보 처리로 구현되는 목적을 고려하여 적절한 경우에 그러하다. 과학적 목적을 위한 개인정보 처리도 임상 실험에 관한 것 등 기타 관련 법률을 준수해야 한다.

(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) 연구원들은 기록부(registries)로부터의 정보를 연결하여 혈관계 질환, 암, 우울증 등의 널리 알려진 의학적 상태에 대한 매우 귀중한 신지식을 얻을 수 있다. 기록부를 토대로 더 많은 인구를 이용할수록, 연구 결과는 향상될 수 있다. 사회과학 내에서, 기록부에 기반을 둔 연구를 통해 연구원들은 실업 및 교육 등 다수의 사회적 조건과 기타 삶의 조건간의 장기적 상관관계에 대한 필수 지식을 얻는다. 기록부를 통해 얻은 연구 결과는 지식이 기반이 된 정책의 수립 및 시행을 위한 근거가 되고, 다수의 삶의 질을 높이며, 사회 서비스의 효율성을 개선시킬 수 있는 확고한 양질의 지식을 제공한다. 과학적 연구를 용이하게 하기 위해, 유럽연합 또는 회원국 법률에 규정된 적절한 조건 및 안전조치에 따라 과학적 연구의 목적으로 개인정보가 처리될 수 있다.

(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

(158) 유지보존의 목적으로 개인정보가 처리되는 경우, 본 규정이 망자에게는 적용되지 않아야 한다는 점을 유념하여 유지보존을 목적으로 한 정보처리에도 본 규정을 적용해야 한다. 공익을 위한 기록을 보유한 공공기관, 공공기구 또는 민간기구는, 유럽연합이나 회원국 법률에 따라, 일반적인 공익을 위해 지속적 가치가 있는 열람을 획득, 보존, 평가, 조성, 기술(describe), 전달, 증진, 유포 및 제공할 법적 의무가 있는 (공공)서비스여야 한다. 회원국은 예를 들어, 과거 전체주의 국가 체제 하의 정치적 행위, 집단 학살, 홀로코스트 등의 비인도적 범죄, 또는 전쟁 범죄에 관한 특정 정보를 제공할 목적으로, 유지보존의 목적을 위한 개인정보의 추가적 처리를 규정할 권한이 있어야 한다.

state regimes, genocide, crimes against humanity, in particular the Holocaust, or war crimes.

(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) 과학적 연구의 목적으로 개인정보가 처리되는 경우, 본 규정은 그 같은 정보처리에도 적용되어야 한다. 본 규정의 취지를 위해, 과학적 연구 목적의 개인정보 처리는 기술의 발전과 실증, 기초연구, 응용연구 및 민간 투자 연구 등을 포괄하는 광범위한 방식으로 해석되어야 한다. 또한, 유럽연합 기능에 관한 조약(TFEU) 제179조에 따라 European Research Area(ERA)를 유지보존하려는 유럽연합의 목적이 고려되어야 한다. 과학적 연구 목적에는 공중보건 분야에서 공익을 위해 시행된 연구도 포함되어야 한다. 과학적 연구의 목적으로 개인정보를 처리하는 특수성에 부합하기 위해, 과학적 연구 목적에서의 개인정보의 발표나 다른 방식으로의 공개에 관한 것 등 특정 조건이 적용되어야 한다. 보건 분야 등에서의 과학적 연구 결과가 정보주체의 이익을 위한 추가적 조치의 사유를 제공하는 경우, 그 같은 조치를 고려하여 본 규정의 통칙이 적용되어야 한다.

(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) 역사적 연구 목적으로 개인정보가 처리되는 경우, 본 규정은 그 같은 정보처리에도 적용되어야 한다. 여기에는 본 규정이 망자에는 적용되지 않아야 한다는 점을 유념하여 역사 연구 및 계보학 목적의 연구도 포함되어야 한다.

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

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

(161) 임상 실험의 과학 연구 활동 참여에 동의할 목적으로, 유럽의회 및 각료이사회 규정서 (EU) No 536/2014의 관련 조문이 적용되어야 한다.

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

(162) 통계 목적으로 개인정보가 처리되는 경우, 본 규정은 그 같은 정보처리에도 적용되어야 한다. 유럽연합 또는 회원국 법률은 본 규정의 한도 내에서 통계 내용, 접근(access) 통제, 통계 목적의 개인정보 처리에 대한 세부사항 및 정보주체의 권리와 자유를 보호하고 통계의 신뢰성을 보장하기 위한 적절한 조치를 결정해야 한다. 통계 목적은 통계 조사나 통계 결과를 작성하는데 필요한 개인정보의 수집 및 처리의 작업 일체를 의미한다. 그 통계 결과는 과학적 연구 목적 등 다른 목적을 위해 추가적으로 활용될 수 있다. 통계 목적에는 통계 목적으로의 정보처리 결과가 개인정보가 아닌 집합체 데이터 (aggregate data)이며 이 결과나 개인정보가 다른 특정 개인에 관한 조치나 결정을 지지하는데 활용되지 않는다는 점이 내포되어 있다.

(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[1] provides further specifications on statistical confidentiality for European statistics.

[1] 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).

(163) 유럽연합과 회원국 통계청이 유럽 및 회원국의 공식적 통계를 작성하기 위해 수집하는 기밀 정보는 보호되어야 한다. 유럽연합의 통계는 유럽연합 기능에 관한 조약(TFEU) 제338조(2)에 규정된 통계 원칙에 부합하여 개발, 작성 및 유포되어야 하고 회원국 통계 또한 회원국 법률을 준수하여야 한다. 유럽의회 및 각료이사회 규정서 (EC) No 223/2009는 유럽연합 통계에 있어 통계의 신뢰성에 대한 추가 세부사항을 규정하고 있다.

(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) 감독기관이 정보처리자나 수탁처리자로부터 개인정보를 열람하고 그들의 부지에 접근할 권리를 획득하는 권한과 관련하여, 회원국은 개인정보 보호권과 직업상의 기밀유지 의무 간의 균형을 유지하는데 요구되는 한, 본 규정의 한도 내에서 직업상의 또는 기타 상응하는 기밀유지 의무를 보호하기 위한 특정 규정을 법률로써 채택할 수 있다. 이는 유럽연합 법률이 요구할 경우 직업상의 기밀유지에 대한 규정을 채택해야 하는 기존의 회원국의 의무를 침해하지 않는다.

(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) 본 규정은 유럽연합 기능에 관한 조약(TFEU) 제17조에 인지된 현행 헌법 하에서의 회원국의 교회 및 종교단체나 공동체의 지위를 존중하고 이를 침해하지 않는다.

(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 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) 개인의 기본권과 자유 및 개인정보 보호권을 보호하고 유럽연합 내에서 개인정보의 자유로운 이전을 보장하기 위한 본 규정의 목적을 충족시키기 위해, 유럽연합 기능에 관한 조약(TFEU) 제290조에 따라 법률을 채택할 권한이 집행위원회에 위임되어야 한다. 특히 인증 메커니즘을 위한 기준 및 요건, 표준화 된 아이콘으로 제시되는 정보, 및 그 같은 아이콘을 제공하는 절차에 관해 위임법률이 채택되어야 한다. 집행위원회가 전문가 차원에서 등 예비 작업 동안에 적절한 자문을 시행하는 것이 특히 중요하다. 집행위원회는 위임법률을 준비하고 작성할 때, 관련 문서가 동시적으로 때맞춰 적절하게 유럽의회와 각료이사회로 전송되도록 해야 한다.

(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) 본 규정의 시행에 대한 균일한 조건을 보장하기 위해, 본 규정이 규정할 시, 집행위원회에 시행 권한이 부여되어야 한다. 그 같은 권한은 규정서 (EU) No 182/2011에 따라 행사되어야 한다. 이러한 정황에서 집행위원회는 영세기업과 중소기업을 위한 특정 조치를 고려해야 한다.
(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) 정보처리자와 수탁처리자 간 및 수탁처리자 간에 체결된 표준계약조항·행동강령·기술표준 및 인증 메커니즘·제3국, 해당 제3국의 영토나 지정 부문, 또는 국제기구가 제공하는 적절한 보호수준· 정보보호표준조항·의무적 기업규칙에 대해 정보처리자·수탁처리자·감독기관 간에 전자적 수단으로 정보를 교환하기 위한 양식과 절차, 상호지원, 감독기관 간, 그리고 감독기관과 유럽정보보호이사회 간에 전자적 수단으로 정보를 교환하기 위한 방식(arrangements)에 대한 시행법률을 채택하기 위해 검토절차가 활용되어야 한다.
(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) 집행위원회는 가용 증거를 통해 제3국, 해당 제3국의 영토나 지정 부문 또는 국제기구가 적절한 보호수준을 보장하지 않음이 입증되고 시급성의 필수적 근거로 요구되는 경우, 즉시 적용 가능한 시행법률을 채택해야 한다.
(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) 유럽연합 전역에 동등한 개인의 보호수준 및 개인정보의 자유로운 이동을 보장하기 위한 본 규정의 목적이 회원국에 의해 충분히 충족될 수 없고 조치의 규모나 효과의 이유로 유럽연합 차원에서 더 원활히 충족될 수 있으므로, 유럽연합은 유럽연합에 관한 협약(TEU) 제5조에 규정된 보완성의 원칙에 따른 조치를 채택할 수 있다. 그 조문에 규정된 비례성의 원칙에 따라, 본 규정은 그 목적을 충족시키는데 필요한 것 이상을 요구하지 않는다.
(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	(171) 지침 95/46/EC는 본 규정에 의해 폐기되어야 한다. 본 규정의 적용일에 이미 시행 중인 정보처리는 본 규정의 발효 후 2년의 기간 내에 본 규정에 따르도록 되어야 한다. 정보처리가 지침 95/46/EC에 따른 동의를 기반으로 할 때, 정보주체는 동의가 주어진 방식이 본 규정의 조건에 부합하는 경우, 정보처리자가 본 규정의 적용일 이후에 그 같은 정보처리를 계속하도록 허락하는 동의를 다시 제공할 필요가 없다. 지침 95/46/EC를 근거로 채택된 집행위원회 결정과 감독기관의 인가는 개정, 대체 또는 폐기될 때까지 효력을 갖는다.

or repealed.	
(172) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on 7 March 20121.	(172) 유럽개인정보보호담당기구는 규정서 (EC) No 45/2001 제28조(2)에 따라 자문을 의뢰받았고 2012년 3월 7일 의견서를 전달하였다.
(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[1], 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) 본 규정서는 개인정보 처리에 관한 기본권 및 자유의 보호에 관련되고 정보처리자의 의무와 개인의 권리 등 유럽의회 및 각료이사회 지침 2002/58/EC에 규정된 동일한 목적을 가진 특정 의무의 적용을 받지 않는 모든 사안에 적용되어야 한다. 본 규정과 지침 2002/58/EC 간의 관계를 명확히 하기 위해, 해당 지침이 적절히 개정되어야 한다. 본 규정이 채택되는 대로, 특히 본 규정과의 일관성을 보장하기 위해 지침 2002/58/EC가 검토되어야 한다.
[1] 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).	
HAVE ADOPTED THIS REGULATION:	본 규정을 채택하였음:

CHAPTER I GENERAL PROVISIONS	제I장 일반 규정
Article 1 **Subject-matter and objectives**	**제1조** **주제 및 목적**
1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.	1. 본 규정은 개인정보의 처리에 있어 자연인을 보호하기 위한 규칙과 개인정보의 자유로운 이동에 관한 규칙에 대하여 규정한다.
2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.	2. 본 규정은 자연인의 자유와 기본권, 특히 개인정보 보호에 대한 권리를 보호한다.
3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.	3. 유럽연합 내에서 개인정보의 자유로운 이동은, 개인정보를 처리함에 있어 자연인의 보호와 연관되어 있다는 이유로, 제한되거나 금지되어서는 안 된다.
Article 2 **Material scope**	**제2조** **물적 범위**
1. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.	1. 본 규정은 전적 또는 부분적으로 자동화 방식에 의해 이루어지는 개인정보의 처리와 자동화 수단 이외의 방식에 의한 것으로서 파일시스템을 구성하거나 구성하기 위한 개인정보의 처리에 적용된다.
2. This Regulation does not apply to the processing of personal data: (a) in the course of an activity which falls outside the scope of Union law; (b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU; (c) by a natural person in the course of a purely personal or household activity; (d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences, the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.	2. 본 규정은 다음 각 호에 해당하는 개인정보의 처리에는 적용되지 않는다. (a) 유럽연합 법률의 범위를 벗어나는 활동 중에 이루어지는 처리 (b) 회원국이 유럽연합 조약(TEU) 제5편, 제2장의 범위에 해당하는 활동을 수행할 때 이루어지는 처리 (c) 자연인이 순수하게 개인활동 또는 가정활동을 하는 중에 이루어지는 처리 (d) 공공의 안녕을 수호하고 이에 대한 위협을 예방하는 등 범죄의 예방, 조사, 적발, 기소 및 형벌 집행의 목적으로 관계당국에 의해 이루어지는 처리
3. For the processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EC) No 45/2001 applies. Regulation (EC) No 45/2001 and other Union legal acts	3. 유럽연합 산하기관, 기구, 사무소 및 에이전시의 개인정보 처리에 대해서는 규정 45/2001/EC가 적용된다. 규정 45/2001/EC 및 그러한 개인정보의 처리에 적용 가능한 기타 유럽연합 법률은 제98조에 따라 본 규

applicable to such processing of personal data shall be adapted to the principles and rules of this Regulation in accordance with Article 98.	정의 원칙 및 규칙에 맞게 조정되어야 한다.
4. This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.	4. 본 규정은 지침 2000/31/EC의 적용, 특히 동 지침의 제12조부터 제15조까지에 규정된 중개서비스 사업자의 책임 규칙이 적용되는 것을 침해해서는 안 된다.
Article 3 **Territorial scope**	**제3조** **영토의 범위**
1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.	1. 본 규정은 유럽연합 역내의 개인정보처리자 또는 수탁처리자의 사업장의 활동에 수반되는 개인정보의 처리에 적용되고, 이 때 해당 처리가 유럽연합 역내 또는 역외에서 이루어지는지 여부는 관계없다.
2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.	2. 본 규정은 개인정보의 처리가 다음 각 호와 관련되는 경우, 유럽연합 역내에 설립되지 않은 개인정보처리자 또는 수탁처리자가 유럽연합 역내에 거주하는 개인정보주체의 개인정보를 처리할 때도 적용된다. (a) 개인정보주체가 지불을 해야 하는지에 관계없이 유럽연합 역내의 개인정보주체에게 재화와 용역을 제공 (b) 유럽연합 역내에서 발생하는 개인정보주체의 행태를 모니터링
3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.	3. 본 규정은 유럽연합 역내에 설립되지 않았으나 국제 공법에 의해 회원국의 법률이 적용되는 장소에 설립된 개인정보주체가 개인정보를 처리하는 데 적용된다.
Article 4 **Definitions**	**제4조** **정의**
For the purposes of this Regulation:	본 규정의 취지에 따르면
(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;	(1) 개인정보는 식별된 또는 식별 가능한 자연인('개인정보주체')과 관련한 일체의 정보를 가리킨다. 식별가능한 자연인은 직접 또는 간접적으로, 특히 이름, 식별번호, 위치정보, 온라인 식별자를 참조하거나 해당인의 신체적, 심리적, 유전적, 정신적, 경제적, 문화적 또는 사회적 정체성에 특이한 하나 이상의 요인을 참조함으로써 식별될 수 있는 자를 가리킨다.
(2) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data,	(2) 처리는 자동화 수단에 의한 것인지 여부에 관계없이 단일의 또는 일련의 개인정보에 행해지는 단일 작업이나 일련의 작업으로서, 수집, 기록,

whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;	편집(organisation), 구성, 저장, 가공 또는 변경(adaptation or alteration), 검색(retrieval), 참조(consultation), 사용, 이전을 통한 제공, 배포나 기타 방식으로의 제공(dissemination or otherwise making available), 연동이나 연계(alignment or combination), 제한, 삭제 또는 파기 등이 이에 해당한다.
(3) 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;	(3) 처리의 제한은 장래의 처리를 제한할 목적으로, 저장된 개인정보에 표시하는 행위를 의미한다.
(4) 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;	(4) 프로파일링은 특히 자연인의 업무 성과, 경제적 상황, 건강, 개인적 선호, 관심사, 신뢰도, 행태, 위치 또는 이동에 관한 측면을 분석하거나 예측하기 위해 행해지는 경우로서, 자연인에 관련한 개인적인 특정 측면을 평가하기 위해 개인정보를 사용하여 이루어지는 모든 형태의 자동화된 개인정보의 처리를 가리킨다.
(5) 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;	(5) 가명처리는 추가적인 정보의 사용 없이는 더 이상 특정 개인정보주체에게 연계될 수 없는 방식으로 개인정보를 처리하는 것이다. 단, 그 같은 추가 정보는 별도로 보관하고, 기술 및 관리적 조치를 적용하여 해당 개인정보가 식별된 또는 식별될 수 있는 자연인에 연계되지 않도록 해야 한다.
(6) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;	(6) 파일링시스템은 기능적 또는 지리학적으로 중앙에 집중되거나 분산되었는지 여부에 관계없이 특정 기준에 따라 열람 가능한 일련의 구조화된 개인정보를 가리킨다.
(7) 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;	(7) 개인정보처리자는 단독으로 또는 제3자와 공동으로 개인정보 처리의 목적 및 방법을 결정하는 자연인 또는 법인, 공공기관, 기관, 기타 기구를 가리킨다. 그러한 처리의 목적 및 방법이 유럽연합 또는 회원국 법률로 결정되는 경우 개인정보처리자 또는 개인정보처리자 지정을 위한 구체적 기준은 유럽연합 또는 회원국 법률로 규정될 수 있다.
(8) 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;	(8) 수탁처리자는 개인정보처리자를 대신하여 개인정보를 처리하는 자연인이나 법인, 공공기관, 기관 또는 기타 기구를 가리킨다.
(9) 'recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;	(9) 수령인은 제3자 포함 여부에 관계없이 개인정보가 제공되는 자연인 또는 법인, 공공기관, 기관, 기타 기구를 가리킨다. 그러나 유럽연합 또는 회원국 법률에 따라 특정 조회업무를 수행하는 체제에서 개인정보를 수령할 수 있는 공공당국은 수령인으로 간주하지 않는다. 그러한 공공당국의 그 같은 개인정보의 처리는 처리 목적에 따라 적용 가능한 개인정보 보호 규칙을 준수하여야 한다.

(10) 'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;	(10) 제3자는 개인정보주체, 개인정보처리자, 수탁처리자, 개인정보처리자나 수탁처리자의 직권에 따라 개인정보를 처리할 수 있는 자를 제외한 자연인이나 법인, 공공기관, 기관 또는 기구를 가리킨다.
(11) 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;	(11) 개인정보주체의 동의는 본인과 관련된 개인정보의 처리에 대해 합의한다는 개인정보주체의 희망을 진술 또는 명백한 적극적인 행위를 통해 자유롭고, 구체적으로, 결과에 대해 인지하여 분명하게 나타낸 의사표시를 가리킨다.
(12) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;	(12) 개인정보 침해는 이전 또는 저장되거나 기타 방식으로 처리된 개인정보가 우발적 또는 불법적으로 파기, 유실, 변경, 무단제공, 무단열람을 초래하게 되는 보안 위반을 가리킨다.
(13) 'genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;	(13) 유전정보는 자연인의 생리나 건강에 관해 고유한 정보를 제공하는 해당인의 선천적 또는 후천적인 유전자 특성과 관련한 개인정보로서, 특히 해당 자연인의 생물학적 샘플 분석을 통해 획득하게 된다.
(14) 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;	(14) 생체정보는 안면 영상이나 지문정보와 같이 특정 기술 처리로 얻어진 자연인의 신체적, 생리적, 행태적 특성과 관련된 정보로서, 자연인을 고유하게 식별할 수 있도록 해주거나 확인해주는 것을 의미한다.
15) 'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;	(15) 건강에 관한 정보는 의료서비스 제공 등 자연인의 신체적 또는 정신적 건강과 관련한 개인정보를 가리키며, 해당인의 건강 상태에 관한 정보를 드러낸다.
(16) 'main establishment' means: (a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment; (b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the	(16) 주 사업장은 다음 각 호를 의미한다. (a) 하나 이상의 유럽연합 회원국에 사업장을 운영하는 개인정보처리자의 경우, 유럽연합 역내의 중앙 행정 지점을 주 사업장으로 본다. 유럽연합 역내의 또 다른 사업장에서 개인정보의 처리 목적 및 처리 방식을 결정하거나, 또 다른 사업장에서 개인정보의 처리 목적 및 처리 방식을 결정하게 할 집행권을 보유하고 있는 경우에는 또 다른 사업장을 주 사업장으로 본다. (b) 하나 이상의 유럽연합 회원국에 사업장을 운영하는 수탁처리자의 경우, 유럽연합 역내의 중앙 행정 지점을 주 사업장으로 본다. 수탁처리자가 유럽연합 역내에 중앙 행정 지점을 가지고 있지 않은 경우에는, 수탁처리자에게 본 규정에 따른 특정 의무가 부과되는 범위 내에서 주요 처리 활동이 이루어지는 사업장을 주 사업장으로 본다.

processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;	
(17) 'representative' means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;	(17) 대리인은 제27조에 따라 개인정보처리자나 수탁처리자가 서면으로 지정하여 유럽연합 역내에 설립된 자연인 또는 법인으로서 본 규칙에 의거, 개인정보처리자 또는 수탁처리자 각각의 의무에 대해 그들을 대신한다.
(18) 'enterprise' means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;	(18) 기업(enterprise)은 정례적으로 경제활동에 종사하는 합명회사, 조합 등 법적 형태와는 상관없이, 경제활동에 종사하는 자연인 또는 법인을 의미한다.
(19) 'group of undertakings' means a controlling undertaking and its controlled undertakings;	(19) 사업체 집단(group of undertakings)은 관리하는 사업체와 그 관리를 받는 사업체를 의미한다.
(20) 'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;	(20) 의무적 기업규칙(binding corporate rules)은 공동 경제활동에 종사하는 사업체 집단 또는 기업체 집단 내부에서 단일 또는 복수의 제3국에 위치한 개인정보처리자나 수탁처리자에게 개인정보를 이전하기 위해, 유럽연합 회원국 영토에 설립된 개인정보처리자 또는 수탁처리자가 준수하는 개인정보 정책을 의미한다.
(21) 'supervisory authority' means an independent public authority which is established by a Member State pursuant to Article 51;	(21) 감독기관(supervisory authority)은 제51조에 따라 유럽연합 회원국이 설립한 독립적인 공공기관을 의미한다.
(22) 'supervisory authority concerned' means a supervisory authority which is concerned by the processing of personal data because: (a) the controller or processor is established on the territory of the Member State of that supervisory authority; (b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or (c) a complaint has been lodged with that supervisory authority;	(22) 처리에 관여하는 감독기관을 의미한다. (a) 해당 감독기관이 소재한 회원국의 영토에 개인정보처리자나 수탁처리자가 설립되는 경우 (b) 해당 감독기관이 소재한 회원국에 거주하는 개인정보주체가 처리로 인해 상당한 영향을 받거나 받을 것으로 예상되는 경우 (c) 해당 감독기관에 민원이 제기된 경우
(23) 'cross-border processing' means either: (a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or	(23) 회원국간 처리(cross-border processing)는 다음 각 호의 하나에 해당한다. (a) 개인정보처리자나 수탁처리자가 하나 이상의 회원국에 설립된 경우로서, 유럽연합 역내에 개인정보처리자나 수탁처리자가 소재한 하나 이상의 회원국에서 사업장의 활동 중에 발생하는 개인정보의 처리

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

(b) 유럽연합 역내의 개인정보처리자나 수탁처리자의 단일 사업장의 활동 중에 발생하지만 하나 이상의 회원국의 개인정보주체에게 상당한 영향을 미치거나 미칠 것으로 예상되는 개인정보의 처리

(24) 'relevant and reasoned objection' means an objection as to whether there is an infringement of this Regulation or not, or whether the envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;

(24) 타당하고 합당한 이의제기는 본 규정에 대한 위반이 존재하는지 여부 또는 개인정보처리자나 수탁처리자와 관련해 예정된 작업이 본 규정을 준수하는지 여부에 대한 이의제기로서, 개인정보주체의 기본적 권리 및 자유, 그리고 해당하는 경우 유럽연합 내의 개인정보의 자유로운 이동에 관한 가결정(draft decision)이 초래하는 위험의 중대성을 명확히 보여준다.

(25) 'information society service' means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council1;

(25) 정보사회 서비스(information society service)는 유럽의회 및 각료이사회 지침(EU) 2015/1535의 제1조 제(1)항 (b)호에서 정의하는 서비스를 의미한다.

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

(26) 국제기구란 국제 공법이 준용되는 조직 및 산하기관, 또는 둘 이상의 국가 간의 협정에 의하거나 이를 기반으로 설립된 모든 기타 기관을 가리킨다.

CHAPTER II
PRINCIPLES

제II장
원칙

Article 5
Principles relating to processing of personal data

제5조
개인정보 처리 원칙

1. Personal data shall be:

1. 개인정보는:

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

(a) 개인정보주체에 대해 적법하고, 공정하며, 투명하게 처리되어야 한다('적법성, 공정성, 투명성').

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

(b) 구체적이고 명시적이며 적법한 목적을 위해 수집되어야 하고, 해당 목적과 양립되지 않는 방식으로 추가 처리되어서는 안 된다. 공익적 기록보존의 목적, 과학적 또는 역사적 연구 목적, 또는 통계적 목적을 위한 추가 처리는 제89조(1)에 따라 본래의 목적과 양립되지 않는 것으로 보지 않는다('목적 제한').

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

(c) 처리되는 목적과 관련하여 적절하고, 타당하며, 필요한 정도로만 제한되어야 한다('데이터 최소화').

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data

(d) 정확해야 하고, 필요한 경우 최신의 것이어야 한다. 처리 목적과 관련하여 부정확한 개인정보는 지체 없이 삭제 또는 정정되도록 모든 적절한 조치가 시행되어야 한다('정확성').

(e) 처리목적 달성에 필요한 기간 동안만 개인정보주체를 식별할 수 있는 형태로 보관되어야 한다. 개인정보는 제89조(1)에 따라 개인정보

that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

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

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

주체의 권리 및 자유를 보호하기 위해 본 규정이 요구하는 적절한 기술 및 관리적 조치를 시행하여 공익적 기록 보존 목적, 과학적 또는 역사적 연구 목적, 통계적 목적을 위해 처리되는 경우 더 오랜 기간 동안 보관될 수 있다.

(f) 개인정보의 적절한 보안을 보장하는 방식으로 처리해야 한다. 보장 방식은, 적절한 기술 및 관리적 조치를 사용하여, 개인정보가 무단으로 또는 불법적으로 처리된다거나 우발적으로 소실, 파기, 손상되었을 경우의 보호조치 등을 포함한다('무결성과 기밀성').

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

2. 개인정보처리자는 제1항이 준수되도록 할 책임이 있으며, 이를 입증할 수도 있어야 한다('책임성').

Article 6
Lawfulness of processing

제6조
처리의 적법성

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

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

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

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

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

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

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

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

1. 개인정보 처리는 적어도 다음 각 호의 하나에 해당되고 그 범위에서만 적법하다.

(a) 개인정보주체가 하나 이상의 특정 목적에 대해 본인의 개인정보 처리를 동의한 경우

(b) 개인정보주체가 계약 당사자가 되는 계약을 이행하거나 계약 체결 전 개인정보주체가 요청한 조치를 취하기 위해 처리가 필요한 경우

(c) 개인정보처리자의 법적 의무를 준수하는데 개인정보 처리가 필요한 경우

(d) 개인정보주체 또는 제3자의 생명에 관한 이익을 보호하기 위해 개인정보 처리가 필요한 경우

(e) 공익을 위하거나 개인정보처리자의 공식권한을 행사하여 이루어지는 업무수행에 처리가 필요한 경우

(f) 개인정보처리자 또는 제3자의 정당한 이익 목적을 위해 처리가 필요한 경우로서, 개인정보가 보호되어야 할 개인정보주체의 이익 또는 기본적 권리와 자유가 우선되는 경우는 제외한다. 개인정보주체가 어린이인 경우에는 특히 그러하다.

제1항 (f)호는 공공기관이 소관 업무를 수행하기 위해 개인정보를 처리하는 경우에는 적용되지 않는다.

2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.	2. 회원국은 본 규정의 규칙을 적용하기 위하여 더욱 구체적인 조문을 유지하거나 도입할 수 있다. 이는 개인정보 처리를 위한 구체적 요건과, 제IX장에서 규정하는 특정 처리 상황 등과 같이 적법하고 공정한 처리를 보장하기 위한 여타 조치들을 더욱 엄밀히 결정함으로써 제1항 (c)호 및 (e)호의 준수를 담보하기 위한 내용에 관한 것이다.
3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by: (a) Union law; or (b) Member State law to which the controller is subject. The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.	3. 제1항의 (c)호 및 (e)호에서의 개인정보 처리의 근거는 다음 각 호를 통해 규정되어야 한다. (a) 유럽연합 법률 (b) 개인정보처리자에게 적용되는 유럽연합 회원국의 법률 처리목적은 상기의 법적 근거에 의해 결정되어야 한다. 제1항 (e)호의 처리는 공익을 위하거나 개인정보처리자의 공식권한을 행사하여 이루어지는 업무수행에 필요한 것이다. 해당 법적 근거로는 본 규정의 규칙을 적절히 적용하기 위한 특정 조문이 있을 수 있으며, 특히, 개인정보처리자의 개인정보 처리 적법성에 대한 일반적인 조건, 해당 처리의 대상이 되는 개인정보의 유형, 관련 개인정보주체, 관련 개인정보의 제공 대상 및 목적, 목적 제한, 보관기간, 제IX장에서 규정하는 특정 처리상황을 위한 조치 등 합법적이고 공정한 처리를 보장하는 조치를 포함한 처리 작업 및 처리절차가 이에 해당한다. 유럽연합 또는 회원국 법률은 공익의 목적을 달성하고 추구하는 적법한 목표에 비례해야 한다.
4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia: (a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing; (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller; (c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10; (d) the possible consequences of the intended further	4. 개인정보를 수집한 목적 외로 처리하는 것이 개인정보주체의 동의 또는 제23조(1)의 목적을 보장하기 위한 민주사회의 필요하고 비례적인 조치를 구성하는 유럽연합 또는 회원국 법률에 근거하지 않는 경우, 개인정보처리자는 개인정보의 목적 외 처리가 해당 개인정보를 수집한 당초 목적과 양립될 수 있는지 확인하기 위해서 특히 다음 각 호를 고려해야 한다. (a) 수집 목적과 의도된 추가처리 목적 간의 연관성 (b) 특히 개인정보주체와 개인정보처리자 간의 관계와 관련해서 등의 개인정보가 수집된 상황 (c) 특히 제9조에 따른 특정 범주의 개인정보가 처리되는지 여부 또는 제10조에 따른 범죄경력 및 범죄행위와 관련한 개인정보가 처리되는지 여부 등 개인정보의 성격 (d) 의도된 추가처리가 개인정보주체에 초래할 수 있는 결과 (e) 암호처리나 가명처리 등 적절한 안전조치의 존재

processing for data subjects; (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.	
Article 7 **Conditions for consent**	**제7조** **동의의 조건**
1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.	1. 처리가 동의를 기반으로 이루어지는 경우, 개인정보처리자는 개인정보주체가 본인의 개인정보 처리에 동의하였음을 입증할 수 있어야 한다.
2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.	2. 개인정보주체의 동의가 기타의 사안과도 관련된 서면의 진술서로 제공되는 경우, 동의 요청은 그 기타의 사안과 분명히 구별되는 방식으로, 이해하기 쉽고 입수가 용이한 형태로, 명확하고 평이한 문구를 사용한 방식으로 제시되어야 한다. 진술서의 어느 부분이라도 본 규정을 위반하는 경우 그 구속력이 인정되지 않는다.
3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw consent as to give it.	3. 개인정보주체는 언제든지 본인의 동의를 철회할 권리를 가진다. 동의의 철회는 철회 이전에 동의를 기반으로 한 처리의 적법성에 영향을 미치지 않는다. 개인정보주체는 동의를 제공하기 전에 이 사실에 대해 고지받아야 한다. 동의의 철회는 동의의 제공만큼 용이해야 한다.
4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.	4. 동의가 자유롭게 제공되는지 여부를 평가할 때, 무엇보다 서비스 제공 등의 계약의 이행이 해당 계약의 이행에 필요하지 않은 개인정보의 처리에 대한 동의를 조건으로 하는지 여부를 최대한 고려해야 한다.
Article 8 **Conditions applicable to child's consent in relation to information society services**	**제8조** **정보사회 서비스와 관련하여 아동의 동의에 적용되는 조건**
1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.	1. 제6조(1)의 (a)호가 적용되는 경우, 아동에게 직접 이루어지는 정보사회 서비스 제공과 관련하여 아동의 개인정보의 처리는 해당 아동이 최소 16세 이상인 경우에 적법하다. 아동이 16세 미만인 경우, 그 같은 처리는 해당 아동의 친권을 보유한 자가 동의를 제공하거나 승인한 경우에만 적법하다. 회원국은 상기의 목적에 대한 아동의 연령을 법률로서 낮추어 규정할 수 있으나, 해당 연령이 13세 미만이 되어서는 안 된다.
2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration	2. 그 같은 경우 개인정보처리자는 가용한 기술을 고려하여 해당 아동의 친권을 보유한 자가 동의를 제공하거나 승인하였는지를 입증하기 위한 합당한 노력을 기울여야 한다.

available technology.	
3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.	3. 제1항은 아동과 관련한 계약의 유효성, 형식 또는 효력에 대한 규정 등 회원국의 일반 계약 법률에 영향을 미칠 수 없다.
Article 9 **Processing of special categories of personal data**	**제9조** **특정 범주의 개인정보의 처리**
1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.	1. 인종 또는 민족, 정치적 견해, 종교적 또는 철학적 신념, 노동조합의 가입여부를 나타내는 개인정보의 처리와 유전자 정보, 자연인을 고유하게 식별할 목적의 생체정보, 건강정보, 성생활 또는 성적 취향에 관한 정보의 처리는 금지된다.
2. Paragraph 1 shall not apply if one of the following applies: (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject; (c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent; (d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects; (e) processing relates to personal data which are manifestly made public by the data subject; (f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; (g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the	2. 다음 각 호의 하나에 해당하는 경우 제1항은 적용되지 않는다. (a) 개인정보주체가 단일 또는 복수의 특정한 목적으로 특정 범주의 개인정보를 처리하는 데 명백한 동의를 제공한 경우. 단, 유럽연합 또는 회원국 법률이 개인정보주체가 제1항의 금지조항을 무효화할 수 없다고 명시적으로 규정하는 경우는 제외된다. (b) 고용, 사회보장, 사회보호법 분야에서 개인정보처리자나 개인정보주체의 의무를 이행하고 특정 권리를 행사하기 위한 목적으로 처리가 필요한 경우. 단, 그 처리는 유럽연합 또는 회원국 법률이나 개인정보주체의 기본적 권리 및 이익에 대한 적절한 안전조치를 규정하는 회원국 법률에 따라 체결된 단체협약에 의해 승인되어야 한다. (c) 개인정보주체가 신체적으로 또는 법률적으로 동의를 제공할 수 없는 경우로서 개인정보주체 또는 제3자의 생명의 이익을 보호하는 데 처리가 필요한 경우 (d) 정치적, 철학적, 종교적 또는 노동조합적 목적을 지닌 재단, 협회, 기타 비영리기관이 적절한 안전조치를 갖추어 수행하는 합법적인 활동의 과정에서 개인정보를 처리하는 경우로서, 해당 처리가 그 목적에 맞게 관련 기관의 회원 또는 이전 회원 또는 관련 기관과 정기적으로 접촉하는 자에 한하여 이루어지고, 개인정보주체의 동의 없이 이러한 개인정보를 기관 외부에 제공하지 않는다는 조건에 따라 수행되는 경우 (e) 개인정보주체가 명백히 공개한 개인정보와 관련된 처리인 경우 (f) 법적 권리의 확립, 행사, 방어를 위하거나 법원이 사법권을 행사할 때마다 처리가 필요한 경우 (g) 추구하는 목표에 비례하도록 유럽연합 또는 회원국 법률에 근거하여 상당한 공익상의 이유로 처리가 필요한 경우와 개인정보보호권의 본질을 존중하고 개인정보주체의 기본적 권리 및 이익을 보호하기 위해 적절하고 구체적인 조치를 제공하는 경우 (h) 예방의학 또는 직업의학의 목적으로 처리가 필요한 경우 및 피고용인의 업무능력 평가, 의학적 진단, 의료서비스 또는 사회복지 또는 치료의 제공, 또는 유럽연합 또는 회원국 법률에 근거하거나 의료전문가와의 계약에 의거하고 제3항의 조건 및 안전조치에 따라 의료 또는 사회복지 제도나 서비스의 관리를 위해 처리가 필요한 경우 (i) 회원국 간의 중대한 건강 위협으로부터 보호하거나 의료서비스·의약

essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

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

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

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

품·의료장비의 높은 품질과 안정성을 보장하는 등 공중보건 분야에서 공익상의 이유로, 특히 직무상의 기밀 등 개인정보주체의 권리와 자유를 보호하기 위해 적절하고 구체적인 조치를 규정하는 유럽연합 또는 회원국 법률에 근거하여 처리가 필요한 경우

(j) 추구하는 목적에 비례하고, 개인정보보호권의 본질을 존중하며, 개인정보주체의 기본적 권리 및 이익을 보호하기 위해 적절하고 구체적인 조치를 제공하는 유럽연합 또는 회원국 법률에 근거하여, 제89조(1)에 따라 공익적 기록보존 목적, 과학적 또는 역사적 연구 목적, 또는 통계적 목적을 위해 처리가 필요한 경우.

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

3. 제1항의 개인정보는 제2항 (h)호의 목적을 위해 처리될 수 있는데, 유럽연합 또는 회원국 법률이나 관련 국가기관이 제정한 규정에 따라 직무상 기밀 유지의 의무가 있는 전문가의 책임에 의하거나 책임 하에서 해당 개인정보가 처리되는 경우나, 유럽연합 또는 회원국 법률이나 관련 국가기관이 수립한 규정에 따라 기밀 유지의 의무가 있는 제3자에 의해 해당 개인정보가 처리되는 경우와 같은 때이다.

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

4. 회원국은 유전정보, 생체정보 또는 건강에 관한 정보에 대하여 제한 등의 추가 조건을 유지하거나 도입할 수 있다.

Article 10
Processing of personal data relating to criminal convictions and offences

제10조
범죄경력 및 범죄행위에 관한 개인정보의 처리

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

범죄경력 및 범죄행위 또는 제6조(1)에 근거한 보안조치와 관련한 개인정보의 처리는 공공기관의 규제 하에서만 수행될 수 있거나, 해당 처리가 개인정보주체의 권리와 자유를 위한 적절한 안전조치를 규정하는 유럽연합 또는 회원국 법률에 승인되는 경우 수행될 수 있다. 종합 범죄경력 기록은 공공기관의 규제 하에서만 보관될 수 있다.

Article 11 **Processing which does not require identification**	**제11조** **신원확인을 요하지 않는 개인정보의 처리**
1. If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.	1. 개인정보처리자가 개인정보를 처리하는 목적상 개인정보주체의 신원확인을 요구하지 않거나 더 이상 요구하지 않아도 되는 경우, 그 개인정보처리자는 본 규정을 준수할 목적에 한하여 개인정보주체를 식별하기 위한 추가 정보를 유지, 취득, 처리할 의무를 가지지 않는다.
2. Where, in cases referred to in paragraph 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 15 to 20 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.	2. 본 조 제1항에 규정된 사례의 경우 개인정보처리자가 개인정보주체를 식별할 수 없음을 입증할 수 있다면, 제15조부터 제20조까지의 조문은 적용되지 않는다. 단, 개인정보주체가 해당 조문에 따라 본인의 권리를 행사하기 위한 목적으로 본인의 신원을 확인할 수 있는 추가 정보를 제공하는 경우는 예외로 한다.
CHAPTER III **RIGHTS OF THE DATA SUBJECT**	**제III장** **개인정보주체의 권리**
SECTION 1 **TRANSPARENCY AND MODALITIES**	**제1절** **투명성 및 형식**
Article 12 **Transparent information, communication and modalities for the exercise of the rights of the data subject**	**제12조** **개인정보주체의 권리 행사를 위한 투명한 정보, 통지 및 형식**
1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.	1. 개인정보처리자는 처리와 관련한 제13조 및 제14조에 명시된 일체의 정보, 제15조부터 제22조까지의 조문 및 제34조에 규정된 일체의 통지를 정확하고, 투명하며, 이해하기 쉬운 형식으로 명확하고 평이한 언어를 사용하여 개인정보주체에게 제공하기 위한 적절한 조치를 취해야 하고, 특히 아동을 특정 대상으로 할 때 더욱 그러해야 한다. 해당 정보는 서면이나 적절한 경우, 전자수단 등 기타 수단을 이용하여 제공되어야 한다. 개인정보주체가 요청하는 경우, 다른 수단을 통해 개인정보주체의 신원이 입증되면, 해당 정보는 구두로 제공될 수 있다.
2. The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.	2. 개인정보처리자는 제15조부터 제22조까지의 조문에 따라 개인정보주체의 권리 행사를 용이하게 해야 한다. 제11조(2)의 경우에서 개인정보처리자는 제15조부터 제22조까지의 조문에 따라 본인의 권리를 행사하려는 개인정보주체의 요청을 거절해서는 안 되며, 개인정보처리자가 개인정보주체를 식별할 수 없음을 입증하는 경우는 예외로 한다.

3. The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.	3. 개인정보처리자는 요청을 접수한 후, 한 달 이내에 부당한 지체 없이, 제15조에서 제22조까지의 조문에 따른 요청에 따라 취해진 조치에 대한 정보를 개인정보주체에게 제공해야 한다. 해당 요청의 복잡성과 요청 횟수를 참작하여 필요한 경우 해당 기간을 2개월 간 더 연장할 수 있다. 개인정보처리자는 요청 접수 후 한 달 이내에 개인정보주체에게 기간 연장 및 지연 사유에 대해 고지하여야 한다. 개인정보주체가 전자양식의 수단으로 요청을 하는 경우, 개인정보주체로부터 별도의 요청이 있지 않는 한, 해당 정보는 가능한 전자양식으로 제공되어야 한다.
4. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.	4. 개인정보처리자가 개인정보주체의 요청에 대해 조치를 취하지 않는 경우, 개인정보주체에게 지체 없이 통지해야 하고 요청의 접수 후 최대 한 달 이내에 조치를 취하지 않은 사유 및 감독기관에 민원을 제기하고 사법 구제를 받을 수 있는 가능성에 대해 개인정보주체에게 고지해야 한다.
5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either: (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or (b) refuse to act on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.	5. 제13조 및 제14조에 명시된 정보와 제15조부터 제22조까지의 조문 및 제34조에 따른 일체의 통지와 조치는 무상으로 제공되어야 한다. 개인정보주체의 요청이 명백하게 근거가 없거나 과도한 경우, 특히 요청이 반복될 경우, 개인정보처리자는 다음 각 호의 하나에 따를 수 있다. (a) 관련 정보 또는 통지를 제공하거나 요청한 조치를 취하는 데 소요되는 행정적 비용을 참작하여 합리적인 비용을 부과한다. (b) 해당 요청에 대한 응대를 거부한다. 개인정보처리자는 해당 요청이 명백하게 근거가 없거나 과도하다는 사실을 입증할 책임이 있다.
6. Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.	6. 제15조에서 제19조까지의 조문에 규정된 요청을 하는 개인의 신원과 관련하여 합리적인 의심이 드는 경우, 개인정보처리자는 제11조를 침해하지 않고 개인정보주체의 신원을 확인하는 데 필요한 추가적 정보 제공을 요청할 수 있다.
7. The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.	7. 제13조 및 제14조에 따라 개인정보주체에게 제공되는 정보는 예정된 처리에 대해 유의미한 개요를 제공하고자 표준화된 아이콘과 결합하여 가시적이고 이해하기 쉬우며 가독성이 뛰어난 방식으로 제공될 수 있다. 해당 아이콘이 전자 방식으로 제공되는 경우, 이는 기계 판독이 가능해야 한다.
8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of determining the information to be presented by the icons and the procedures for providing standardised icons.	8. 집행위원회는 아이콘으로 제시되는 정보 및 표준 아이콘의 제공 절차를 결정하기 위한 목적으로 제92조에 따라 위임 법률을 채택할 권한을 갖는다.

SECTION 2
INFORMATION AND ACCESS TO PERSONAL DATA

Article 13
Information to be provided where personal data are collected from the data subject

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

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

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

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

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

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

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

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

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

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

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

제2절
정보 및 개인정보 열람

제13조
개인정보가 개인정보주체로부터 수집되는 경우 제공되는 정보

1. 개인정보주체에 관련된 개인정보를 개인정보주체로부터 수집하는 경우, 개인정보처리자는 개인정보를 취득할 당시 개인정보주체에게 다음 각 호의 정보 일체를 제공해야 한다.

   (a) 개인정보처리자 또는 해당되는 경우, 개인정보처리자의 대리인의 신원 및 상세 연락처

   (b) 해당되는 경우, 개인정보보호 담당관의 상세 연락처

   (c) 해당 개인정보의 예정된 처리의 목적뿐 아니라 처리의 법적 근거

   (d) 제6조(1)의 (f)호에 근거한 처리의 경우, 개인정보처리자 또는 제3자의 정당한 이익

   (e) 해당되는 경우, 개인정보의 수령인 또는 수령인의 범주

   (f) 해당되는 경우, 개인정보처리자가 제3국이나 국제기구의 수령인에게 개인정보를 이전할 예정이라는 사실과 집행위원회가 내린 적정성 결정의 유무, 또는 제46조, 제47조, 제49조(1)의 두 번째 단락에 명시된 이전의 경우, 적절하고 적합한 안전조치, 그 사본을 입수하기 위한 수단, 안전조치가 사용 가능하게 되는 경우에 대한 언급

2. 제1항의 정보와 함께, 개인정보처리자는 개인정보가 입수될 때 공정하고 투명한 처리를 보장하는 데 필요한, 다음 각 호의 추가 정보를 개인정보주체에 제공해야 한다.

   (a) 개인정보의 보관기간, 또는 이것이 여의치 않을 경우, 해당 기간을 결정하는 데 사용하는 기준

   (b) 개인정보처리자에게 본인의 개인정보에 대한 열람, 정정, 삭제를 요구하거나 개인정보주체 본인에 관한 처리의 제한이나 반대를 요구할 권리, 그리고 본인의 개인정보를 이전할 수 있는 권리의 유무

   (c) 해당 처리가 제6조(1)의 (a)호나 제9조(2)의 (a)호에 근거하는 경우, 철회 이전에 동의를 기반으로 하는 처리의 적법성에 영향을 주지 않고 언제든지 동의를 철회할 수 있는 권리의 유무

   (d) 감독기관에 민원을 제기할 수 있는 권리

   (e) 개인정보의 제공이 법정 또는 계약상의 요건이거나 계약 체결에 필요한 요건인지의 여부 및 개인정보주체가 개인정보를 제공할 의무가 있는지의 여부, 그리고 해당 정보를 제공하지 않을 경우 발생할 수

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

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

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

있는 결과

(f) 제22조(1) 및 (4)에 규정된 프로파일링 등, 자동화된 의사결정의 유무. 최소한 이 경우, 관련 논리에 관한 유의미한 정보와 그 같은 처리가 개인정보주체에 미치는 중대성 및 예상되는 결과

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

3. 개인정보처리자가 개인정보를 수집한 목적 외로 추가 처리할 예정인 경우, 개인정보처리자는 추가 처리 이전에, 개인정보주체에게 해당하는 기타 목적에 관한 정보와 제2항의 관련 추가 정보 일체를 제공해야 한다.

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

4. 개인정보주체가 이미 관련 정보를 보유하고 있는 경우, 제1항, 제2항 및 제3항은 적용되지 않는다.

Article 14
Information to be provided where personal data have not been obtained from the data subject

제14조
개인정보가 개인정보주체로부터 수집되지 않은 경우 제공되는 정보

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

(a) the identity and the contact details of the controller and, if any, of the controller's representative;

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

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

(d) the categories of personal data concerned;

(e) the recipients or categories of recipients of the personal data, where applicable;

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

1. 개인정보가 개인정보주체로부터 수집되지 않은 경우, 개인정보처리자는 다음 각 호의 정보를 개인정보주체에게 제공해야 한다.

(a) 개인정보처리자 또는 가능한 경우, 개인정보처리자의 대리인의 신원 및 상세 연락처

(b) 해당되는 경우, 개인정보보호 담당관의 상세 연락처

(c) 해당 개인정보의 예정된 처리 목적뿐 아니라 처리의 법적 근거

(d) 관련 개인정보의 범주

(e) 해당되는 경우, 개인정보의 수령인 또는 수령인의 범주

(f) 해당되는 경우, 개인정보처리자가 제3국이나 국제기구의 수령인에게 개인정보를 이전할 예정이라는 사실과 집행위원회가 내린 적정성 결정의 유무, 또는 제46조, 제47조, 제49조(1)의 두 번째 단락에 명시된 이전의 경우, 적절하고 적합한 안전조치, 그 사본을 입수하기 위한 수단, 안전조치가 사용 가능하게 되는 경우에 대한 언급

2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject: (a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period; (b) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party; (c) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability; (d) where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal; (e) the right to lodge a complaint with a supervisory authority; (f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources; (g) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.	2. 제1항의 정보와 함께, 개인정보처리자는 개인정보주체와 관련한 공정하고 투명한 처리를 보장하는 데 필요한, 다음 각 호의 정보를 개인정보주체에 제공해야 한다. (a) 개인정보의 보관기간, 또는 이것이 여의치 않을 경우, 해당 기간을 결정하는 데 사용하는 기준 (b) 제6조(1)의 (f)호에 근거한 처리의 경우, 개인정보처리자 또는 제3자의 정당한 이익 (c) 개인정보처리자에게 본인의 개인정보에 대한 열람, 정정, 삭제를 요구하거나 개인정보주체 본인에 관한 처리의 제한이나 반대를 요구할 권리, 그리고 본인의 개인정보를 이전할 수 있는 권리의 유무 (d) 해당 처리가 제6조(1)의 (a)호나 제9조(2)의 (a)호에 근거하는 경우, 철회 이전에 동의를 기반으로 한 처리의 적법성에 영향을 주지 않고 언제든지 동의를 철회할 수 있는 권리의 유무 (e) 감독기관에 민원을 제기할 수 있는 권리 (f) 개인정보의 출처, 가능한 경우 해당 개인정보가 공개 출처로부터 비롯되었는지 여부 (g) 제22조(1) 및 (4)에 규정된 프로파일링 등, 자동화된 의사결정의 유무. 최소한 이 경우, 관련 논리에 관한 유의미한 정보와 그 같은 처리가 개인정보주체에 미치는 중대성 및 예상되는 결과
3. The controller shall provide the information referred to in paragraphs 1 and 2: (a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed; (b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or (c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.	3. 개인정보처리자는 제1항 및 제2항에 명시된 정보를 다음 각 호와 같이 제공해야 한다. (a) 개인정보가 처리된 특정 상황과 관련하여 개인정보를 입수한 후 최소 한 달 이내의 합리적인 기간 내 (b) 개인정보가 개인정보주체에게 통지할 목적으로 사용되는 경우, 최소한 해당 정보주체에 최초로 통지한 시점 (c) 제3의 수령인에게 개인정보의 제공이 예상되는 경우, 최소한 개인정보가 최초로 제공되는 시점
4. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.	4. 개인정보처리자가 수집 목적 이외의 목적으로 개인정보를 추가 처리하려는 경우, 해당 개인정보처리자는 추가 처리 이전에 개인정보주체에게 해당되는 기타의 목적에 대한 정보와 제2항에 규정된 관련 추가 정보의 일체를 제공해야 한다.
5. Paragraphs 1 to 4 shall not apply where and insofar as:	5. 다음 각 호에 해당하는 경우 그 범위에 한하여 제1항부터 제4항까지가

(a) the data subject already has the information;

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

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

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

적용되지 않는다.

(a) 개인정보주체가 이미 해당 정보를 보유하고 있는 경우

(b) 해당 정보의 제공이 불가능하다고 입증되거나 비례적으로 과도한 노력을 요하는 경우, 특히 제89조(1)의 조건 및 안전조치에 따른 공익적 기록보존 목적, 과학적 또는 역사적 연구 목적, 또는 통계적 목적을 위한 처리에 대해 그러한 경우. 또는 본 조 제1항에 규정된 의무가 그 처리의 목적 달성을 불가능하게 하거나 중대하게 손상시킬 것으로 예상되는 경우. 그 경우, 개인정보처리자는 개인정보주체에게 통보해야 할 정보를 공개하는 등 개인정보주체의 권리와 자유 및 정당한 이익을 보호하기 위한 적정한 조치를 취해야 한다.

(c) 개인정보처리자가 준수해야 하고, 개인정보주체의 정당한 이익을 보호하는 데 적절한 조치를 규정하는 유럽연합 또는 회원국 법률이 취득 또는 제공을 명확히 규정하는 경우

(d) 법정 기밀유지의 의무 등, 유럽연합 또는 회원국 법률이 규제하는 직무상 기밀유지의 의무에 따라, 해당 개인정보가 기밀로 남아있어야 하는 경우.

Article 15
Right of access by the data subject

제15조
개인정보 주체의 열람권

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

   (a) the purposes of the processing;

   (b) the categories of personal data concerned;

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

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

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

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

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

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

1. 개인정보주체는 본인에 관련된 개인정보가 처리되고 있는지 여부에 관련해 인정보처리자로부터 확답을 얻을 권리를 가지며, 이 경우, 개인정보 및 다음 각 호의 정보에 대한 열람권을 가진다.

   (a) 처리 목적

   (b) 관련된 개인정보의 범주

   (c) 개인정보를 제공받았거나 제공받을 수령인 또는 수령인의 범주, 특히 제3국 또는 국제기구의 수령인

   (d) 가능한 경우, 개인정보의 예상 보관 기간 또는, 여의치 않은 경우, 해당 기간을 결정하는 데 사용되는 기준

   (e) 개인정보처리자에게 본인의 개인정보에 대한 정정 또는 삭제를 요구하거나 개인정보주체 본인에 관한 처리의 제한이나 반대를 요구할 권리

   (f) 감독기관에 민원을 제기할 수 있는 권리

   (g) 개인정보주체로부터 개인정보를 수집하지 않은 경우, 개인정보의 출처에 대한 모든 가용한 정보

   (h) 제22조(1) 및 (4)에 규정된 프로파일링 등 자동화된 의사결정의 유무. 최소한 이 경우, 관련 논리에 관한 유의미한 정보와 그 같은 처리가 개인정보주체에 가지는 중대성 및 예상되는 결과

consequences of such processing for the data subject.	
2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.	2. 개인정보가 제3국이나 국제기구로 이전되는 경우, 개인정보주체는 제46조에 따라 적절한 안전조치에 대해 고지 받을 권리가 있다.
3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.	3. 개인정보처리자는 처리가 진행 중인 개인정보의 사본을 제공해야 한다. 개인정보주체가 추가 사본을 요청하는 경우, 개인정보처리자는 행정적 비용에 근거하여 합리적인 비용을 청구할 수 있다. 개인정보주체가 전자적 방식으로 해당 요청을 하는 경우, 관련 정보는 통상적으로 사용되는 전자적 양식으로 제공되어야 한다.
4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.	4. 제3항에 규정된 사본을 입수할 권리는 제3자의 권리와 자유를 침해하지 않아야 한다.
SECTION 3 **RECTIFICATION AND ERASURE**	**제3절** **정정 및 삭제**
Article 16 **Right to rectification**	**제16조** **정정권**
The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her . Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.	개인정보 주체는 본인에 관하여 부정확한 개인정보를 부당한 지체 없이 정정하도록 개인정보처리자에게 요구할 권리를 가진다. 개인정보주체는 처리 목적을 참작하여 추가 진술을 제공할 수단을 통하는 등, 불완전한 개인정보를 보완할 권리를 가진다.
Article 17 **Right to erasure ('right to be forgotten')**	**제17조** **삭제권('잊힐 권리')**
1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds	1. 개인정보 주체는 본인에 관한 개인정보를 부당한 지체 없이 삭제하도록 개인정보처리자에게 요청할 권리를 가지며, 개인정보처리자는 다음 각 호가 적용되는 경우, 부당한 지체 없이 개인정보를 삭제할 의무를 가진다. (a) 개인정보가 수집된, 그렇지 않으면 처리된 목적에 더 이상 필요하지 않은 경우 (b) 개인정보주체가 제6조(1)의 (a)호 또는 제9조(2)의 (a)호에 따라 처리의 기반이 되는 동의를 철회하고, 해당 처리에 대한 기타의 법적 근거가 없는 경우 (c) 개인정보주체가 제21조(1)에 따라 처리에 반대하고 관련 처리에 대해 우선하는 정당한 근거가 없거나, 개인정보주체가 제21조(2)에 따라 처리에 반대하는 경우 (d) 개인정보가 불법적으로 처리된 경우

for the processing, or the data subject objects to the processing pursuant to Article 21(2);

(d) the personal data have been unlawfully processed;

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

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

(e) 개인정보처리자에 적용되는 유럽연합 또는 회원국 법률의 법적 의무를 준수하기 위해 개인정보가 삭제되어야 하는 경우

(f) 제8조(1)에 규정된 정보사회서비스의 제공과 관련하여 개인정보가 수집된 경우

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

2. 개인정보처리자가 개인정보를 공개하고 제1항에 따라 해당 개인정보를 삭제할 의무가 있는 경우, 개인정보처리자는 가용 기술과 시행 비용을 참작하여 개인정보를 처리하는 개인정보처리자에게 개인정보주체가 그 같은 개인정보처리자들에게 해당 개인정보에 대한 링크, 사본 또는 복제본의 삭제를 요청하였음을 고지하기 위한 기술적 조치 등, 적절한 조치를 취해야 한다.

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

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

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

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

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

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

3. 제1항 및 제2항은 다음 각 호를 위해 개인정보의 처리가 필요한 경우에는 적용되지 않는다.

(a) 표현과 정보의 자유에 대한 권리의 행사

(b) 개인정보처리자에 적용되는 유럽연합 또는 회원국 법률의 법적 의무를 준수하는데 처리가 요구되는 경우 또는, 공익을 위해서 또는 개인정보처리자에게 부여된 공적 권한을 행사하여 업무를 수행하는 경우

(c) 제9조(3)뿐만 아니라 제9조(2)의 (h)호 및 (i)호에 따른 공중보건 분야의 공익상의 이유인 경우

(d) 제89조(1)에 따른 공익적 기록보존 목적, 과학적 또는 역사적 연구 목적, 또는 통계적 목적에 해당하는 경우로서, 제1항의 권리가 그 처리의 목적 달성을 불가능하게 하거나 중대하게 손상시킬 것으로 예상되는 경우

(e) 법적 권리의 확립, 행사 또는 방어를 위한 경우

Article 18
Right to restriction of processing

제18조
처리에 대한 제한권

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

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

1. 다음 각 호의 하나에 해당하는 경우, 개인정보주체는 개인정보처리자로부터 처리의 제한을 얻을 권리를 가진다.

(a) 개인정보처리자가 개인정보의 정확성을 증명할 수 있는 기간 동안, 개인정보주체가 해당 개인정보의 정확성에 대해 이의를 제기하는 경우

(b) 처리가 불법적이고 개인정보주체가 해당 개인정보의 삭제에 반대하

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

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

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

고 대신 개인정보에 대한 이용제한을 요청하는 경우

(c) 개인정보처리자가 처리 목적을 위해 해당 개인정보가 더 이상 필요하지 않으나, 개인정보처리자가 법적 권리의 확립, 행사, 방어를 위해 요구하는 경우

(d) 개인정보처리자의 정당한 이익이 개인정보주체의 정당한 이익에 우선하는지 여부를 확인할 때까지, 개인정보주체가 제21조(1)에 따라 처리에 대해 반대하는 경우

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

2. 개인정보의 처리가 제1항에 따라 제한되는 경우, 그 개인정보는, 보관을 제외하고, 개인정보주체의 동의가 있거나 법적 권리의 확립, 행사 또는 방어를 위해, 또는 제3자나 법인의 권리를 보호하거나 유럽연합 또는 회원국의 중요한 공익상의 이유에 한해서만 처리될 수 있다.

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

3. 제1항에 따라 처리의 제한을 취득한 개인정보주체는 처리제한이 해제되기 전에 개인정보처리자로부터 이를 고지 받아야 한다.

Article 19
Notification obligation regarding rectification or erasure of personal data or restriction of processing

제19조
개인정보의 정정이나 삭제 또는 처리의 제한에 관한 고지 의무

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

개인정보처리자는 개인정보를 제공 받은 각 수령인에게 제16조, 제17조(1) 또는 제18조에 따라 이행된 개인정보의 정정이나 삭제 또는 처리의 제한에 대해 통지해야 하며, 이러한 통지가 불가능하다고 입증되거나 과도한 노력을 수반하는 경우는 예외로 한다. 개인정보처리자는 개인정보주체의 요청 시, 개인정보주체에게 해당 수령인에 대해 통지해야 한다.

Article 20
Right to data portability

제20조
개인정보 이전권

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

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

1. 개인정보주체는 개인정보처리자에게 제공한 본인에 관련된 개인정보를 체계적이고, 통상적으로 사용되며 기계 판독이 가능한 형식으로 수령할 권리가 있으며, 개인정보를 제공받은 개인정보처리자로부터 방해 받지 않고 다른 개인정보처리자에게 해당 개인정보를 이전할 권리를 가진다.

(a) 처리가 제6조(1)의 (a)호나 제9조(2)의 (a)호에 따른 동의나 제6조(1)의 (b)호에 따른 계약을 근거로 하는 경우

(b) 처리가 자동화된 수단으로 시행되는 경우

(b) the processing is carried out by automated means.	
2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.	2. 제1항에 따른 본인의 개인정보 이전권을 행사하는 데 있어, 개인정보주체는 기술적으로 가능한 경우 해당 개인정보를 한 개인정보처리자에서 다른 개인정보처리자로 직접 이전할 권리를 가진다.
3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.	3. 본 조 제1항에 규정된 권리의 행사는 제17조를 침해해서는 안 된다. 해당 권리는 공익을 위해서 또는 개인정보처리자에게 부여된 공식권한을 행사하여 이루어지는 업무 수행에 필요한 처리에는 적용되지 않는다.
4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.	4. 제1항에 규정된 권리는 다른 개인의 권리와 자유를 침해하지 않아야 한다.
SECTION 4 **RIGHT TO OBJECT AND AUTOMATED INDIVIDUAL DECISION-MAKING**	**제4절** **반대할 권리 및 자동화된 개별 의사결정**
Article 21 **Right to object**	**제21조** **반대할 권리**
1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on points (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.	1. 개인정보주체는 본인의 특별한 상황에 따라 제6조(1)의 (e)호 및 (f)호에 근거한 프로파일링 등, 본인과 관련한 개인정보의 처리에 대해 언제든지 반대할 권리를 가진다. 개인정보처리자는 개인정보주체의 이익, 권리 및 자유에 우선하는 처리를 위한, 또는 법적 권리의 확립, 행사나 방어를 위한 설득력 있는 정당한 이익을 입증하지 않는 한, 해당 개인정보를 더 이상 처리해서는 안 된다.
2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.	2. 직접 마케팅을 목적으로 개인정보가 처리되는 경우, 개인정보주체는 언제든지 해당 마케팅을 위한 본인에 관한 개인정보의 처리에 반대할 권리가 있으며, 그러한 처리에는 해당 직접 마케팅과 관련된 경우 프로파일링이 포함된다.
3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.	3. 개인정보주체가 직접 마케팅을 위한 처리에 반대하는 경우, 해당 개인정보는 더 이상 그러한 목적으로 처리될 수 없다.
4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.	4. 제1항 및 제2항의 권리는, 아무리 늦어도 개인정보주체에게 처음 고지한 시점에, 명백하게 개인정보주체에게 통지되어야 하며, 명확하고 기타의 정보와는 별도로 제공되어야 한다.

5. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.	5. 정보사회서비스 이용의 환경에서, 또한 지침 2002/58/EC에 관계없이, 개인정보주체는 기술 규격서를 사용한 자동화된 수단을 통해 반대할 권리를 행사할 수 있다.
6. Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.	6. 개인정보가 제89조(1)에 의거한 과학적 또는 역사적 연구 목적이나 통계적 목적을 위해 처리되는 경우로서, 공익을 위한 업무 수행에 필요한 처리가 아닌 경우라면 개인정보주체는 본인과 관련한 특별한 상황에 따라 본인에 관한 개인정보의 처리에 반대할 권리를 가진다.
Article 22 **Automated individual decision-making, including profiling**	**제22조** **프로파일링 등 자동화된 개별 의사결정**
1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.	1. 개인정보주체는 프로파일링 등, 본인에 관한 법적 효력을 초래하거나 이와 유사하게 본인에게 중대한 영향을 미치는 자동화된 처리에만 의존하는 결정의 적용을 받지 않을 권리를 가진다.
2. Paragraph 1 shall not apply if the decision: (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller; (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or (c) is based on the data subject's explicit consent.	2. 결정이 다음 각 호에 해당하는 경우에는 제1항이 적용되지 않는다. (a) 개인정보주체와 개인정보처리자 간의 계약을 체결 또는 이행하는 데 필요한 경우 (b) 개인정보처리자에 적용되며, 개인정보주체의 권리와 자유 및 정당한 이익을 보호하기 위한 적절한 조치를 규정하는 유럽연합 또는 회원국 법률이 허용하는 경우 (c) 개인정보주체의 명백한 동의에 근거하는 경우
3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.	3. 제2항 (a)호 및 (c)호의 사례의 경우, 개인정보처리자는 개인정보주체의 권리와 자유 및 정당한 이익, 최소한 개인정보처리자의 인적 개입을 확보하고 본인의 관점을 피력하며 결정에 대해 이의를 제기할 수 있는 권리를 보호하는 데 적절한 조치를 시행해야 한다.
4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) apply and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.	4. 제2항의 결정은 제9조(2)의 (a)호와 (g)호가 적용되고, 개인정보주체의 권리와 자유 및 정당한 이익을 보호하는 적절한 조치가 갖추어진 경우가 아니라면 제9조(1)의 특정 범주의 개인정보를 근거로 해서는 안 된다.

SECTION 5 RESTRICTIONS	제5절 제한
Article 23 **Restrictions**	**제23조** **제한**
1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard: (a) national security; (b) defence; (c) public security; (d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; (e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security; (f) the protection of judicial independence and judicial proceedings; (g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions; (h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a), (b), (c), (d), (e) and (g); (i) the protection of the data subject or the rights and freedoms of others; (j) the enforcement of civil law claims.	1. 개인정보처리자나 수탁처리자에게 적용되는 유럽연합 또는 회원국 법률은 입법 조치를 통해 제5조뿐만 아니라 제12조부터 제22조까지의 조문과 제34조에 규정된 의무 및 권리의 영역을 제한할 수 있다. 단, 그러한 제한이 기본적 권리 및 자유의 본질을 존중하고 민주사회에서 다음 각 호를 보호하는 데 필요하고 비례적인 조치일 때로 유럽연합 또는 회원국 법률의 조문이 제12조부터 제22조까지의 조문에 규정된 권리 및 의무에 상응하는 경우에 그러하다. (a) 국가안보 (b) 국방 (c) 공공 안보(public security) (d) 공안의 보호 및 공안에 대한 위협의 예방 등 범죄의 예방, 수사, 적발, 또는 형사범죄의 기소나 형벌의 집행 (e) 유럽연합 또는 회원국의 일반적 공익을 위한 기타 중요한 목표로서, 특히 통화, 예산, 과세 현안, 공중보건 및 사회보장 등, 유럽연합 또는 회원국의 중요한 경제적 또는 재정적 이익 (f) 사법 독립성 및 사법 절차에 대한 보호 (g) 규제대상 직종(regulated professions)의 윤리 침해에 대한 예방, 조사, 적발, 기소 (h) (a), (b), (c), (d), (e), (g)호에서 규정된 경우, 부정기적일지라도 공적 권한의 행사와 연계된 모니터링, 점검, 또는 규제기능 (i) 개인정보주체 또는 제3자의 권리와 자유에 대한 보호 (j) 민법 청구의 집행
2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to: (a) the purposes of the processing or categories of processing; (b) the categories of personal data; (c) the scope of the restrictions introduced; (d) the safeguards to prevent abuse or unlawful access or	2. 특히, 제1항의 모든 입법 조치에는 관련이 있는 경우 최소한 다음 각 호에 관한 구체적인 조문이 포함되어야 한다. (a) 처리 또는 처리 범주의 목적 (b) 개인정보의 범주 (c) 도입된 제한의 범위 (d) 남용, 불법 열람 또는 이전을 예방하기 위한 안전조치 (e) 개인정보처리자나 개인정보처리자 범주에 대한 상세설명

transfer;

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

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

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

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

(f) 처리의 성격, 범위 및 처리나 처리 범주의 목적을 고려한 보관기간 및 적용 가능한 안전조치

(g) 개인정보주체의 권리 및 자유에 대한 위험

(h) 제한의 목적을 침해하지 않는다면, 개인정보주체가 제한에 관해 고지 받을 권리

CHAPTER IV
CONTROLLER AND PROCESSOR

제IV장
개인정보처리자와 수탁처리자

SECTION 1
GENERAL OBLIGATIONS

제1절
일반적 의무

Article 24
Responsibility of the controller

제24조
개인정보처리자의 책임

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

1. 개인정보처리자는 개인정보의 처리가 자연인의 권리 및 자유에 미치는 위험의 다양한 가능성 및 정도와 함께 최신 기술, 실행 비용, 그리고 처리의 성격, 범위, 상황 및 목적을 고려하여, 그 처리가 본 규정에 따라 이루어졌음을 보장하고 입증할 수 있도록 적절한 기술 및 관리적 조치를 취해야 한다.

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

2. 처리활동과 관련하여 비례하는 경우, 제1항의 조치는 개인정보처리자의 적절한 개인정보보호 정책의 이행을 포함해야 한다.

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

3. 제40조의 승인된 행동강령의 준수 또는 제42조의 공인 인증 메커니즘은 개인정보처리자의 의무의 준수를 입증하기 위한 요소로 사용될 수 있다.

Article 25
Data protection by design and by default

제25조
설계 및 기본설정에 의한 개인정보보호

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of

1. 개인정보처리자는 개인정보의 처리가 자연인의 권리 및 자유에 미치는 위험의 다양한 가능성 및 정도와 함께 최신 기술, 실행 비용, 그리고 처

processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.	리의 성격, 범위, 상황 및 목적을 고려하여, 가명처리 등의 기술 및 관리적 조치를 개인정보의 처리 방법을 결정한 시점 및 그 처리가 이루어지는 해당 시점에 이행해야 한다. 그러한 기술 및 관리적 조치는 본 규정의 요건을 충족시키고 개인정보주체의 권리를 보호하기 위해 데이터 최소화 등 개인정보보호 원칙을 효율적으로 이행하고 필요한 안전조치를 개인정보처리에 통합할 수 있도록 설계되어야 한다.
2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.	2. 개인정보처리자는 기본설정을 통해 각 특정 처리 목적에 필요한 개인정보만 처리되도록 적절한 기술 및 관리적 조치를 이행해야 한다. 그 의무는 수집되는 개인정보의 양, 그 처리 정도, 보관기관 및 이용가능성에 적용된다. 특히, 그러한 조치는 기본설정을 통해 개인정보가 관련 개인의 개입 없이 불특정 다수에게 열람되지 않도록 한다.
3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.	3. 제42조에 의거한 승인된 인증 메커니즘은 본 조 제1항 및 제2항에 규정된 요건의 준수를 입증하는 요소로 사용될 수 있다.
Article 26 **Joint controllers**	**제26조** **공동 개인정보처리자**
1. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.	1. 두 명 이상의 개인정보처리자가 공동으로 처리의 목적과 방법을 결정하는 경우, 이들은 공동 개인정보처리자가 된다. 공동 정보처리자는 당사자간의 협의를 통해, 본 규정에 따른 책임을 준용, 특히 개인정보주체의 권리 행사에 대한 각자의 책임과 제13조 및 제14조의 정보를 제공할 각자의 임무를 투명하게 결정해야 하되, 그러한 각자의 책임이 개인정보처리자에 적용되는 유럽연합 또는 회원국 법률에 의해 결정되는 경우는 예외로 한다. 그러한 협의를 통해 개인정보주체에 대한 연락담당관을 지정할 수 있다.
2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.	2. 제1항의 협의는 개인정보주체에 대한 공동 개인정보처리자의 개별 역할과 관계를 충분히 반영해야 한다. 해당 협의의 골자를 개인정보주체에 제공해야 한다.
3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.	3. 제1항의 협의의 조건과 관계없이, 개인정보주체는 본 규정에 따라 각 개인정보처리자와 관련하여, 그리고 이들에 반대하여 본인의 권리를 행사할 수 있다.

Article 27 Representatives of controllers or processors not established in the Union	제27조 유럽연합 내에 설립되지 않은 개인정보처리자 또는 수탁처리자의 대리인
1. Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in the Union.	1. 제3조(2)가 적용되는 경우, 개인정보처리자 또는 수탁처리자는 유럽연합 역내 대리인을 서면으로 지정해야 한다.
2. This obligation shall not apply to: (a) processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or (b) a public authority or body.	2. 이 의무는 다음 각 호에 적용되지 않는다. (a) 부정기적인 처리로서, 제9조(1)의 특정 범주의 개인정보의 처리 또는 제10조의 범죄경력 및 범죄행위에 관한 개인정보의 처리가 대규모로 이루어지지 않으며, 처리의 성격, 정황, 범위 및 목적을 고려할 시 자연인의 권리 및 자유에 위험을 초래할 가능성이 없는 경우 (b) 공공당국 또는 기관
3. The representative shall be established in one of those Member States where the data subjects are and whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored.	3. 대리인은 개인정보주체가 거주하고, 재화 또는 용역의 제공과 관련하여 해당 개인정보주체의 개인정보가 처리되거나 행동이 모니터링 되는 회원국 중 한 곳에 설립되어야 한다.
4. The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation.	4. 대리인은 개인정보처리자 또는 수탁처리자에 의해 위임되며, 개인정보처리자 또는 수탁처리자와 함께, 또는 이들을 대신하여 본 규정을 준수하기 위한 목적으로 처리와 관련한 모든 사안에 대해 감독기관 및 개인정보주체와 교섭해야 한다.
5. The designation of a representative by the controller or processor shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves.	5. 개인정보처리자 또는 수탁처리자의 대리인 지정은 개인정보처리자 또는 수탁처리자 본인에게 제기될 수 있는 법적 조치를 침해하지 않아야 한다.
Article 28 Processor	제28조 수탁처리자
1. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.	1. 개인정보처리자를 대신하여 처리가 이루어지는 경우, 개인정보처리자는 적절한 기술 및 관리적 조치 이행을 통해 그 처리가 본 규정의 요건을 충족시키고, 개인정보주체의 권리를 보호하도록 충분한 보증을 제공하는 수탁처리자만 이용해야 한다.
2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the	2. 수탁처리자는 사전의 특정한 또는 일반적인 개인정보처리자의 서면 승인 없이 타 수탁처리자를 고용할 수 없다. 일반적인 서면 승인의 경우, 수탁처리자는 개인정보처리자에게 타 수탁처리자의 추가 또는 대체와 관련한 예정된 변경에 대해 고지하여, 개인정보처리자가 이러한 변경에

addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

반대할 기회를 제공해야 한다.

3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

   (a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

   (b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

   (c) takes all measures required pursuant to Article 32;

   (d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;

   (e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

   (f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;

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

   (h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

   With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

3. 수탁처리자의 처리는 개인정보처리자와 관련하여 수탁처리자에게 구속력을 가지고, 처리의 주제와 지속기간, 처리의 성격과 목적, 개인정보의 유형과 개인정보주체의 범주, 개인정보처리자의 의무와 권리를 규정하는 유럽연합 또는 회원국 법률에 따른 계약이나 기타 법률의 규제를 받는다. 그 계약 또는 기타 법률은 수탁처리자에 대하여 특히 다음 각 호와 같이 규정해야 한다.

   (a) 수탁처리자는 개인정보처리자의 서면 지시에 한하여 개인정보를 처리하며, 여기에는 제 3국 또는 국제기관으로의 개인정보 이전이 포함되며, 유럽연합 또는 수탁처리자에 적용되는 회원국 법률이 요구하는 경우는 제외한다. 이 경우, 수탁처리자는 처리 이전에 해당 법률요건을 개인정보처리자에게 고지해야 하며, 해당 법률이 공익상의 중요한 이유로 그러한 통지를 금지하는 경우는 예외로 한다. 제3국 또는 국제기구로의 개인정보 이전에 관해서 등 개인정보처리자의 문서화된 지시에 한하여 개인정보를 처리하나, 수탁처리자에게 적용되는 유럽연합 또는 회원국 법률로 요구되는 경우는 제외한다.

   (b) 수탁처리자는 개인정보를 처리하도록 승인 받은 개인이 기밀유지를 약속하도록 보장하거나 적절한 법정 기밀유지의 의무를 적용 받도록 한다.

   (c) 제32조에 따라 요구되는 모든 조치를 취한다.

   (d) 타 수탁처리자와 협력하기 위해서 제2항 및 제4항에 규정된 조건을 준수한다.

   (e) 해당 처리의 성격을 참작하여, 제III장에 규정된 개인정보주체의 권리행사의 요청에 대응해야 하는 개인정보처리자의 의무 이행을 위해, 가능한 경우, 적절한 기술 및 관리적 조치를 통해 개인정보처리자를 지원한다.

   (f) 처리의 성격과 수탁처리자에게 가용한 정보를 참작하여, 개인정보처리자가 제32조에서 제36조에 따른 의무를 준수할 수 있도록 지원한다.

   (g) 개인정보처리자의 선택에 따라, 처리와 관련된 서비스의 공급이 종료된 후, 유럽연합 또는 회원국 법률이 해당 개인정보의 보관을 요구하는 경우가 아니라면 모든 관련 개인정보를 삭제하거나 개인정보처리자에게 반환하며, 기존의 사본을 삭제한다.

   (h) 본 조에 규정된 의무의 준수를 입증하는데 필요한 일체의 정보를 개인정보처리자에게 제공하고 점검 등의 개인정보처리자 또는 개인정보처리자가 위임한 타 감사자가 수행하는 감사를 허용하고 이에 기여한다.

   (h) 호와 관련하여, 수탁처리자는 어떠한 지시가 본 규정 또는 기타 유럽연합 또는 회원국의 개인정보보호 조문을 위반한다고 판단되는 경우 즉시 개인정보처리자에게 이에 대해 통지해야 한다.

4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the

4. 수탁처리자가 개인정보처리자를 대신하여 특정 처리 활동을 수행하기 위해 타 수탁처리자와 함께 일하는 경우, 제3항에 규정된 개인정보처리

same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.	자와 수탁처리자 간의 계약 또는 기타 법률에 명시된 동일한 개인정보 보호의 의무는 유럽연합 또는 회원국 법률에 따른 계약이나 기타 법률의 방식으로 관련 타 수탁처리자에게 부과되어야 하며, 특히 해당 처리가 본 규정의 요건을 충족시키는 방식으로 적절한 기술 및 관리적 조치를 이행하는 것에 대해 충분한 보증을 제공해야 한다. 해당 타 수탁처리자가 본인의 개인정보 보호의 의무를 이행하지 않을 경우, 최초의 수탁처리자는 그 수탁처리자의 의무 이행에 대해 개인정보처리자에게 전적인 책임을 져야 한다.
5. Adherence of a processor to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of this Article.	5. 수탁처리자가 제40조의 승인된 행동강령 또는 제42조의 공인 인증 메커니즘을 준수하는 것은 본 조 제1항 및 제4항에 규정된 충분한 보증을 입증하는 요소로 활용될 수 있다.
6. Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in paragraphs 3 and 4 of this Article may be based, in whole or in part, on standard contractual clauses referred to in paragraphs 7 and 8 of this Article, including when they are part of a certification granted to the controller or processor pursuant to Articles 42 and 43.	6. 개인정보처리자와 수탁처리자 간의 개별 계약을 침해하지 않고, 본 조 제3항 및 제4항에 규정된 계약 또는 기타 법률은 전적 또는 부분적으로 본 조 제7항 및 제8항에 규정된 정보보호 표준 계약조항(standard contractual clauses)에 근거할 수 있으며, 해당 계약 및 기타 법률이 제42조 및 제43조에 따라 개인정보처리자 또는 수탁처리자에게 수여된 인증의 일부인 경우에도 그러하다.
7. The Commission may lay down standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the examination procedure referred to in Article 93(2).	7. 집행위원회는 본 조 제3항 및 제4항에 규정된 사안에 대하여, 제93조(2)에 규정된 심사 절차에 따라 정보보호 표준 계약조항을 규정할 수 있다.
8. A supervisory authority may adopt standard contractual clauses for the matters referred to in paragraph 3 and 4 of this Article and in accordance with the consistency mechanism referred to in Article 63.	8. 감독기관은 본 조 제3항 및 제4항에 규정된 사안에 대하여, 제63조에 규정된 일관성 메커니즘에 따라 정보보호 표준 계약조항을 채택할 수 있다.
9. The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form.	9. 제3항 및 제4항에 규정된 계약이나 기타 법률은 전자 양식 등 서면으로 작성되어야 한다.
10. Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.	10. 제82조, 제83조, 제84조를 침해하지 않고, 수탁처리자가 처리의 목적 및 방법을 결정함으로써 본 규정을 위반하는 경우, 수탁처리자는 해당 처리와 관련하여 개인정보처리자로 간주되어야 한다.

Article 29 Processing under the authority of the controller or processor	제29조 개인정보처리자 및 수탁처리자의 권한에 따른 처리
The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.	수탁처리자, 그리고 개인정보처리자나 수탁처리자의 권한에 따라 행하는 자로서 개인정보를 열람할 수 있는 자는 유럽연합 또는 회원국 법률로 요구되는 경우가 아니라면 개인정보처리자의 지시에 따른 경우를 제외하고 해당 개인정보를 처리해서는 안 된다.
Article 30 **Records of processing activities**	**제30조** **처리 활동의 기록**
1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information: (a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer; (b) the purposes of the processing; (c) a description of the categories of data subjects and of the categories of personal data; (d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations; (e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of appropriate safeguards; (f) where possible, the envisaged time limits for erasure of the different categories of data; (g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).	1. 각 개인정보처리자와, 해당하는 경우, 그 개인정보처리자의 대리인은 본인의 책임 하에 진행되는 처리 활동의 기록을 보존해야 한다. 해당 기록은 다음 각 호의 정보를 포함해야 한다. (a) 개인정보처리자와, 해당하는 경우, 공동 개인정보처리자, 개인정보처리자의 대리인 및 개인정보보호담당관의 이름 및 연락처 (b) 처리의 목적 (c) 개인정보주체의 범주 및 개인정보의 범주에 대한 설명 (d) 제3국 또는 국제기구의 수령인 등, 개인정보를 제공받았거나 제공받을 예정인 수령인의 범주 (e) 해당하는 경우, 제3국 및 국제기구의 신원 확인 등, 제3국 또는 국제기구로의 개인정보 이전 및 제49조(1)의 2호에 규정된 이전의 경우에는 적절한 안전조치에 대한 문서 (f) 가능한 경우, 각기 다른 범주의 정보를 삭제하는 데 예상되는 기한 (g) 가능한 경우, 제32조(1)에 규정된 기술 및 관리적 안전조치에 대한 전반적인 설명
2. Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing: (a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer; (b) the categories of processing carried out on behalf of each controller;	2. 각 수탁처리자, 그리고 해당하는 경우 관련 수탁처리자의 대리인은 개인정보처리자를 대신하여 수행하는 전 범주의 처리활동에 대한 기록을 보존해야 하며, 해당 기록은 다음 각 호의 정보를 포함해야 한다. (a) 관련 수탁처리자(들) 및 수탁처리자가 대행하는 각 개인정보처리자의 이름과 연락처, 그리고 해당하는 경우, 개인정보처리자와 수탁처리자의 대리인 및 개인정보담당관의 이름과 연락처 (b) 각 개인정보처리자를 대신하여 수행하는 처리의 범주 (c) 해당하는 경우, 제3국 및 국제기구의 신원 확인 등, 제3국 또는 국제기구로의 개인정보 이전 및 제49조(1)의 2호에 규정된 이전의 경우에는 적절한 안전조치에 대한 문서

(c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of appropriate safeguards; (d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).	(d) 가능한 경우, 제32조(1)에 규정된 기술 및 관리적 안전조치에 대한 전반적인 설명
3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.	3. 제1항 및 제2항에 규정된 기록은 전자 양식 등, 서면으로 작성되어야 한다.
4. The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.	4. 해당 개인정보처리자와 수탁처리자, 그리고 해당하는 경우, 개인정보처리자 또는 수탁처리자의 대리인은 요청이 있을 경우 감독기관에 기록을 제공해야 한다.
5. The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.	5. 제1항 및 제2항에 규정된 의무는 직원 250인 미만의 기업이나 조직에는 적용되지 않는다. 단, 해당 기업이 수행하는 처리가 개인정보주체의 권리와 자유에 위험을 초래할 것으로 예상되거나, 간헐적이지 않거나, 제9조(1)에 규정된 특정 범주의 개인정보를 포함하거나, 제10조에 규정된 범죄경력 및 범죄행위에 관련된 개인정보를 다루는 경우는 예외로 한다.
Article 31 **Cooperation with the supervisory authority**	**제31조** **감독기관과의 협력**
The controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks.	개인정보처리자와 수탁처리자, 그리고 해당하는 경우, 개인정보처리자나 수탁처리자의 대리인은 요청 시 직무를 수행함에 있어 감독기관과 협력해야 한다.
SECTION 2 SECURITY OF PERSONAL DATA	**제2절** **개인정보의 보안**
Article 32 **Security of processing**	**제32조** **처리의 보안**
1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity,	1. 개인정보처리자와 수탁처리자는 개인정보의 처리가 자연인의 권리 및 자유에 미치는 위험의 다양한 가능성 및 정도와 함께 최신 기술, 실행 비용, 그리고 처리의 성격, 범위, 상황 및 목적을 고려하여, 해당 위험에 적정한 보안 수준을 보장하기 위해 특히 다음 각 호 등을 포함하여 적정한 기술 및 관리적 조치를 이행해야 한다. (a) 개인정보의 가명처리 및 암호처리 (b) 처리 시스템 및 서비스의 지속적인 기밀성과 무결성, 가용성, 복원력을 보장할 수 있는 역량

availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

(c) 물리적 또는 기술적 사고가 발생하는 경우 개인정보에 대한 가용성 및 열람을 시의 적절하게 복원 할 수 있는 역량

(d) 처리의 보안을 보장하는 기술 또는 관리적 조치의 효율성을 정기적으로 테스트 및 평가하기 위한 절차

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

2. 보안의 적정 수준을 평가할 때는 처리로 인해 발생하는 위험성, 특히 이전, 저장 또는 다른 방식으로 처리된 개인정보에 대한 우발적 또는 불법적 파기, 유실, 변경, 무단 제공, 무단 열람에 대해 고려해야 한다.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

3. 제40조에 규정된 공인된 행동강령 또는 제42조에 규정된 공식 인증 메커니즘을 준수하는 것은 본 조 제1항에 규정된 요건의 준수를 입증하는 요소로 활용될 수 있다.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

4. 개인정보처리자와 수탁처리자는 개인정보처리자나 수탁처리자의 권한에 따라 개인정보를 열람하는 모든 자연인이 유럽연합 또는 회원국 법률로 요구되는 것이 아니라면 개인정보처리자의 지시에 따른 경우를 제외하고는 개인정보를 처리하지 못하도록 해야 한다.

Article 33
Notification of a personal data breach to the supervisory authority

제33조
감독기관에 대한 개인정보 침해 통지

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

1. 개인정보의 침해가 발생할 경우, 개인정보처리자는 부당한 지체 없이, 가급적 이를 알게 된 후 72시간 내에, 제55조에 따라 감독기관에 해당 개인정보의 침해를 통지해야 한다. 단, 해당 개인정보의 침해가 자연인의 권리와 자유에 위험을 초래할 것으로 예상되지 않는 경우는 예외로 한다. 72시간 내에 감독기관에 이를 통보하지 않을 경우에는 지연 사유를 동봉해야 한다.

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

2. 수탁처리자는 개인정보의 침해를 알게 된 후 부당한 지체 없이 개인정보처리자에게 이를 통지해야 한다.

3. The notification referred to in paragraph 1 shall at least:

(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and

3. 제1항에서 규정한 통지는 최소한 다음 각 호를 포함해야 한다.

(a) 가능하다면 관련 개인정보주체의 범주 및 대략적인 수, 관련 개인정보 기록의 범주 및 대략적인 수 등을 포함한 개인정보 침해의 성격에 대한 설명

approximate number of personal data records concerned; (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; (c) describe the likely consequences of the personal data breach; (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.	(b) 개인정보보호담당관, 그리고 더 많은 정보를 얻을 수 있는 경우, 기타 연락 가능한 개인의 이름 및 상세 연락처 전달 (c) 개인정보 침해로 인해 발생할 수 있는 결과에 대한 설명 (d) 적절한 경우, 개인정보 침해로 인한 부작용을 완화하기 위한 조치 등, 해당 개인정보 침해 해결을 위해 개인정보처리자가 취하거나 취하도록 제안되는 조치에 대한 설명
4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.	4. 정보를 동시에 제공할 수 없는 경우에는 부당한 지체 없이 해당 정보를 단계별로 제공할 수 있다.
5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.	5. 개인정보처리자는 개인정보 침해와 관련된 사실, 유출로 인한 영향, 이에 대해 시행된 시정 조치 등, 모든 개인정보 침해 건을 문서화해야 한다.
Article 34 **Communication of a personal data breach to the data subject**	**제34조** **개인정보주체에 대한 개인정보 침해 통지**
1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.	1. 개인정보의 침해가 자연인의 권리와 자유에 중대한 위험을 초래할 것으로 예상되는 경우, 개인정보처리자는 부당한 지체 없이 개인정보주체에게 그 개인정보 침해에 대해 통지해야 한다.
2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b), (c) and (d) of Article 33(3).	2. 본 조 제1항에 규정된 개인정보주체에 대한 통지에서는 해당 개인정보 유출의 성격을 명확하고 평이한 언어로 기술하고, 최소한 제33조(3)의 (b)호, (c)호, (d)호에 규정된 정보 및 권고를 포함해야 한다.
3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met: (a) the controller has implemented appropriate technical and organisational protection measures, and that those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; (b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;	3. 다음 각 호의 하나에 해당하는 경우, 제1항의 개인정보주체에 대한 통지는 요구되지 않는다. (a) 개인정보처리자가 적절한 기술 및 관리적 보호조치를 시행하였고, 그 조치, 특히 암호처리 등 관련 개인정보를 열람 권한이 없는 개인에게 이해될 수 없도록 만드는 조치가 침해로 영향을 받은 개인정보에 적용된 경우 (b) 개인정보처리자가 제1항에 규정된 개인정보주체의 권리와 자유에 대한 중대한 위험을 더 이상 실현될 가능성이 없도록 만드는 후속 조치를 취한 경우 (c) 필요 이상의 노력이 수반될 수 있는 경우. 이 경우, 공개 또는 유사한 조치를 통해 개인정보주체가 동등하게 효과적인 방식으로 통지받도록 해야 한다.

(c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.	
4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.	4. 개인정보처리자가 개인정보주체에게 개인정보 침해에 대해 아직 통지하지 않은 경우, 관련 감독기관은 중대한 위험을 초래하는 개인정보 침해의 가능성을 고려한 후, 개인정보처리자에게 통지하도록 요구하거나 제3항의 어느 조건이라도 충족시키도록 결정할 수 있다.
SECTION 3 **DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION**	**제3절** **개인정보보호 영향평가 및 사전 자문**
Article 35 **Data protection impact assessment**	**제35조** **개인정보보호 영향평가**
1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.	1. 처리의 성격과 범위, 상황, 목적을 참작하여, 특히 신기술을 사용하는 처리 유형이 개인의 권리와 자유에 중대한 위험을 초래할 것으로 예상되는 경우, 개인정보처리자는 처리 이전에, 예정된 처리 작업이 개인정보 보호에 미치는 영향에 대한 평가를 수행해야 한다. 한 번의 평가로 유사한 중대한 위험을 초래하는 일련의 유사 처리 작업을 다룰 수 있다.
2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.	2. 개인정보처리자는 개인정보보호담당관이 지정된 경우, 개인정보보호 영향평가를 수행할 때, 담당관의 자문을 구해야 한다.
3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of: (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or (c) a systematic monitoring of a publicly accessible area on a large scale.	3. 제1항에 규정된 개인정보보호 영향평가는 특히 다음 각 호의 경우 요구되어야 한다. (a) 프로파일링 등의 자동화된 처리에 근거한, 개인에 관한 개인적 측면을 체계적이고 광범위하게 평가하는 것으로 해당 평가에 근거한 결정이 해당 개인에게 법적 효력을 미치거나 이와 유사하게 개인에게 중대한 영향을 미치는 경우 (b) 제9조(1)에 규정된 특정범주의 개인정보에 대한 대규모 처리나 제10조에 규정된 범죄경력 및 범죄 행위에 관련된 개인정보에 대한 처리 (c) 공개적으로 접근 가능한 지역에 대한 대규모의 체계적 모니터링
4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the	4. 감독기관은 제1항에 따라 개인정보보호 영향평가의 요건이 적용되는 처리 작업의 종류의 목록을 작성 및 공개해야 한다. 감독기관은 제68조에

requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.	규정된 유럽정보보호이사회에 해당 목록을 통보해야 한다.
5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.	5. 감독기관은 개인정보보호 영향평가가 요구되지 않는 처리 작업의 종류의 목록 또한 작성하여 공개할 수 있다. 감독기관은 유럽정보보호이사회에 해당 목록을 통보해야 한다.
6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.	6. 제4항 및 제5항에 규정된 목록을 채택하기 이전에, 관련 감독기관은 해당 목록이 복수의 회원국 내의 개인정보주체에게 재화와 서비스를 제공하거나 그들의 행동을 모니터링 하는 것과 관련된 처리활동에 관계가 있는 경우, 또는 유럽연합 내 개인정보의 자유로운 이동에 상당한 영향을 미칠 수 있는 처리활동과 관련 있는 경우, 제63조에 규정된 일관성 메커니즘을 적용해야 한다.
7. The assessment shall contain at least: (a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes; (c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.	7. 평가는 최소한 다음의 각 호를 포함해야 한다. (a) 예상되는 처리 작업 및 개인정보처리자의 정당한 이익 등 개인정보처리의 목적에 대한 체계적인 설명 (b) 목적과 관련한 처리 작업의 필요성 및 비례성에 대한 평가 (c) 제1항에 규정된 개인정보주체의 권리와 자유에 대한 위험성 평가; (d) 개인정보주체와 기타 관련인의 권리 및 정당한 이익을 고려하여 개인정보의 보호를 보장하고 본 규정의 준수를 입증하기 위한 안전조치, 보안조치, 메커니즘 등 위험성 처리에 예상되는 조치
8. Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.	8. 특히 개인정보보호 영향평가를 위해 관련 개인정보처리자나 수탁처리자가가 수행하는 처리 작업의 영향을 평가할 때는 해당 개인정보처리자나 수탁처리자가 제40조의 승인된 행동강령을 준수하는 것을 고려해야 한다.
9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.	9. 적절한 경우, 개인정보처리자는 상업적 이익이나 공익의 보호 또는 처리작업의 보안을 침해하지 않고, 예정된 처리에 대한 개인정보주체 또는 그 대리인의 의견을 구해야 한다.
10. Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question,	10. 제6조(1)의 (c)호 또는 (e)호에 따른 처리가 개인정보처리자에 적용되는 유럽연합 또는 회원국 법률 내에 법적 근거를 두고 있는 경우로서, 해당 법률이 특정 처리 작업이나 일련의 관련 작업을 규제하고 개인정보보호 영향평가가 이미 그 법적 근거를 채택하는 중에 일반적 영향평가

and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.	의 일환으로 시행된 경우, 제1항에서 제7항까지 적용되지 않는다. 단, 회원국이 처리활동 이전에 이러한 영향평가의 수행이 필요하다고 고려하는 경우는 예외로 한다.
11. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.	11. 필요하다면, 개인정보처리자는 적어도 처리 작업으로 초래되는 위험에 변화가 있을 시에는 처리가 개인정보보호 영향평가에 따라 실시되는지를 평가하기 위한 검토를 시행해야 한다.
Article 36 **Prior consultation**	**제36조** **사전 자문**
1. The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.	1. 제35조에 따른 개인정보보호 영향평가를 통해 처리가 고위험의 결과를 초래하는 경우로서 개인정보처리자가 그 위험을 완화하기 위해 취한 조치가 부재한 것으로 나타나는 경우 해당 처리 전 감독기관의 자문을 구해야 한다.
2. Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the supervisory authority shall, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of its powers referred to in Article 58. That period may be extended by six weeks, taking into account the complexity of the intended processing. The supervisory authority shall inform the controller and, where applicable, the processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay. Those periods may be suspended until the supervisory authority has obtained information it has requested for the purposes of the consultation.	2. 감독기관이 제1항의 예정된 처리가 본 규정을 위반할 것이라는 의견을 제시하는 경우로서 특히 개인정보처리자가 위험을 충분히 파악하거나 완화하지 못한 경우, 감독기관은 자문 요청을 접수한지 8주의 기간 내에 해당 개인정보처리자에게 서면 형식의 권고를 제공해야 하고, 해당하는 경우 수탁처리자에게도 제공해야 하며, 제58조에 규정된 어느 권한이라도 사용할 수가 있다. 해당 기간은 예정된 처리의 복합성을 고려하여 6주까지 연장될 수 있다. 감독기관은 자문 요청을 접수한 후 한 달 내에 개인정보처리자에게, 그리고 해당하는 경우 수탁처리자에게도 지연의 사유와 함께 그 같은 기간 연장에 대해 알려야 한다. 그 기간은 감독기관이 자문의 목적으로 요청한 정보를 입수할 때까지 연기될 수 있다.
3. When consulting the supervisory authority pursuant to paragraph 1, the controller shall provide the supervisory authority with: (a) where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings; (b) the purposes and means of the intended processing; (c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation; (d) where applicable, the contact details of the data protection officer; (e) the data protection impact assessment provided for in Article 35; and	3. 제1항에 따라 감독기관의 자문을 구할 때, 개인정보처리자는 다음 각 호를 감독기관에 제공해야 한다. (a) 가능한 경우, 처리에 관여하는 개인정보처리자, 공동 개인정보처리자 및 수탁처리자의 개별 책임, 특히 사업체집단 내의 처리에 대한 책임 (b) 예정된 처리의 목적 및 방법 (c) 본 규정에 따라 개인정보주체의 권리와 자유를 보호하기 위해 제공되는 조치 및 안전조치 (d) 가능한 경우, 개인정보보호 담당관의 상세 연락처 (e) 제35조에 규정된 개인정보보호 영향평가 (f) 감독기관이 요청한 기타 정보

(f) any other information requested by the supervisory authority.	
4. Member States shall consult the supervisory authority during the preparation of a proposal for a legislative measure to be adopted by a national parliament, or of a regulatory measure based on such a legislative measure, which relates to processing.	4. 회원국은 자국 의회가 채택하는 입법 조치에 대한 제안서 또는 이러한 입법 조치에 근거한 처리에 관련된 규제조치를 준비하는 동안 자문기관의 자문을 구해야 한다.
5. Notwithstanding paragraph 1, Member State law may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health.	5. 제1항에 관계없이, 회원국 법률은 사회 보호 및 공중 보건과 관련된 처리 등, 개인정보처리자가 공익을 위해 소관업무를 수행함에 있어 정보를 처리하는 것과 관련하여, 개인정보처리자가 감독기관에게 자문을 구하고 사전 승인을 획득하도록 요구할 수 있다.
SECTION 4 **DATA PROTECTION OFFICER**	**제4절** **개인정보보호 담당관**
Article 37 **Designation of the data protection officer**	**제37조** **개인정보보호 담당관의 지정**
1. The controller and the processor shall designate a data protection officer in any case where: (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.	1. 다음 각 호에 해당하는 경우, 개인정보처리자와 수탁처리자는 개인정보보호 담당관을 지정해야 한다. (a) 법원이 사법 권한을 행사하는 경우를 제외한 공공당국 또는 기관이 처리를 하는 경우 (b) 개인정보처리자나 수탁처리자의 핵심 활동이 처리의 성격, 범위 또는 목적에 의해 개인정보주체에 대한 정기적이고 체계적인 대규모의 모니터링을 요하는 처리 작업들로 구성되는 경우 (c) 개인정보처리자 또는 수탁처리자의 핵심 활동이 제9조에 따른 특정 범주의 개인정보와 제10조에 규정된 범죄경력 및 범죄 행위에 관련된 개인정보를 대규모로 처리하는 것으로 구성되는 경우
2. A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.	2. 사업체 집단은 단일의 개인정보보호 담당관을 지정할 수 있는데, 각 사업장이 해당 개인정보보호 담당관을 쉽게 이용할 수 있는 경우에 그러하다.
3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.	3. 개인정보처리자 또는 수탁처리자가 공공당국이나 기관인 경우, 조직의 구조나 규모를 고려하여, 다수의 그러한 당국이나 기관을 위해 단일의 개인정보보호 담당관이 지정될 수 있다.
4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or,	4. 제1항에 규정된 것 이외의 경우, 개인정보처리자나 수탁처리자의 각 범주를 대표하는 협회 또는 기타 기관은, 유럽연합 또는 회원국 법률이 요구하는 경우, 개인정보보호 담당관을 지정할 수 있거나 지정해야 한다.

where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.	개인정보보호 담당관은 개인정보처리자 또는 수탁처리자를 대변하는 해당 협회 및 기타 기관을 대행할 수 있다.
5. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.	5. 개인정보보호 담당관은 직무상의 자질, 특히 개인정보보호법과 실무에 대한 전문가적 지식과 제39조에 규정된 업무를 수행할 수 있는 능력에 근거하여 지정되어야 한다.
6. The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.	6. 개인정보보호 담당관은 개인정보처리자 또는 수탁처리자의 직원일 수 있거나, 서비스계약에 근거하여 업무를 수행할 수 있다.
7. The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.	7. 개인정보처리자 또는 수탁처리자는 개인정보보호 담당관의 상세 연락처를 공개하며 이를 감독기관에 통보하여야 한다.
Article 38 **Position of the data protection officer**	**제38조** **개인정보보호 담당관의 지위**
1. The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.	1. 개인정보처리자 및 수탁처리자는 개인정보보호 담당관이 개인정보 보호와 관련된 모든 문제에 적절하고 시의 적절하게 관여하도록 해야 한다.
2. The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.	2. 개인정보처리자 및 수탁처리자는 개인정보보호 담당관이 제39조의 업무를 수행하고 개인정보 및 처리 작업을 열람하며 전문지식을 유지하는 데 필요한 자원을 제공함으로써 그의 업무 수행을 지원해야 한다.
3. The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.	3. 개인정보처리자 또는 수탁처리자는 개인정보보호 담당관이 그 업무의 수행에 있어 어떠한 지시도 받지 않도록 보장해야 한다. 개인정보보호 담당관은 본인의 업무 수행을 이유로 개인정보처리자나 수탁처리자에 의해 해임 또는 처벌받아서는 안 된다. 개인정보보호 담당관은 개인정보처리자 또는 수탁처리자의 최고 경영진에게 직접 보고해야 한다.
4. Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.	4. 개인정보주체는 본인의 개인정보 처리 및 본 규정에 따른 권리 행사와 관련한 모든 사안에 관해 개인정보보호 담당관에 연락을 취할 수 있다.
5. The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.	5. 개인정보보호 담당관은 유럽연합이나 회원국 법률에 따라 본인의 업무 수행에 관해 비밀 또는 기밀유지의 의무를 준수해야 한다.

6. The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.	6. 개인정보보호 담당관은 기타 업무 및 직무를 수행할 수 있다. 개인정보처리자나 수탁처리자는 이러한 업무 및 직무가 이해의 상충을 초래하지 않도록 해야 한다.
Article 39 **Tasks of the data protection officer**	**제39조** **개인정보보호 담당관의 업무**
1. The data protection officer shall have at least the following tasks: (a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions; (b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits; (c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35; (d) to cooperate with the supervisory authority; (e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.	1. 개인정보보호 담당관은 최소한 다음 각 호의 업무를 수행하여야 한다. (a) 개인정보처리자나 수탁처리자, 그리고 처리를 수행하는 직원에게 본 규정과 유럽연합 또는 회원국의 개인정보보호 규정에 따른 의무에 대해 고지 및 권고 (b) 책임 할당, 인식 제고, 처리 작업에 관련된 직원 교육 및 관련 감사 등 본 규정, 기타 유럽연합 또는 회원국의 개인정보보호 규정, 개인정보 보호와 관련한 개인정보처리자 또는 수탁처리자의 정책이 준수되는지 모니터링 (c) 요청이 있을 경우, 제35조에 따라 개인정보보호 영향평가에 관한 자문 제공 및 평가의 이행을 모니터링 (d) 감독기관과 협력 (e) 제36조에 규정된 사전 자문 등, 처리에 관련한 현안에 대해 감독기관의 연락처의 역할 수행 및 적절한 경우, 기타 사안에 대한 자문 제공
2. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.	2. 개인정보보호 담당관은 업무를 수행할 때 처리의 성격과 범위, 상황, 목적을 참작하여 처리 작업과 연계된 위험을 충분히 고려해야 한다.
SECTION 5 **CODES OF CONDUCT AND CERTIFICATION**	**제5절** **행동강령 및 인증**
Article 40 **Codes of conduct**	**제40조** **행동강령**
1. The Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.	1. 회원국, 감독기관, 유럽정보보호이사회, 집행위원회는 다양한 처리 부문의 명확한 특징과 영세 및 중소기업의 특정 요구를 고려하여 본 규정을 적절히 적용하기 위한 취지의 행동강령을 입안하도록 장려한다.
2. Associations and other bodies representing categories of	2. 개인정보처리자나 수탁처리자의 각 범주를 대표하는 협회(associations)

controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to: (a) fair and transparent processing; (b) the legitimate interests pursued by controllers in specific contexts; (c) the collection of personal data; (d) the pseudonymisation of personal data; (e) the information provided to the public and to data subjects; (f) the exercise of the rights of data subjects; (g) the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained; (h) the measures and procedures referred to in Articles 24 and 25 and the measures to ensure security of processing referred to in Article 32; (i) the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects; (j) the transfer of personal data to third countries or international organisations; or (k) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79.	또는 기타 기관은 다음 각 호와 관련하여 본 규정의 적용을 구체화할 목적으로 행동강령을 제정하거나 해당 강령을 수정 또는 확대할 수 있다. (a) 공정하고 투명한 처리 (b) 특정 상황에서의 개인정보처리자의 정당한 이익 (c) 개인정보의 수집 (d) 개인정보의 가명처리 (e) 일반 및 개인정보주체에게 제공되는 정보 (f) 개인정보주체의 권리 행사 (g) 아동에게 제공되는 정보 및 아동의 보호, 아동에 대한 친권을 보유한 자의 동의를 획득하는 방식 (h) 제24조 및 제25조에 규정된 조치 및 절차, 제32조에 규정된 처리의 안전을 보장하기 위한 조치 (i) 감독기관 및 개인정보주체에게 개인정보 침해에 대해 통지 (j) 제3국이나 국제기구로 개인정보 이전 (k) 제77조 및 제79조에 따른 개인정보주체의 권리를 침해하지 않고, 처리와 관련하여 개인정보처리자와 개인정보주체 간의 분쟁을 해결하기 위한 재판 외 절차 및 기타 분쟁해결 절차
3. In addition to adherence by controllers or processors subject to this Regulation, codes of conduct approved pursuant to paragraph 5 of this Article and having general validity pursuant to paragraph 9 of this Article may also be adhered to by controllers or processors that are not subject to this Regulation pursuant to Article 3 in order to provide appropriate safeguards within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (e) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards including with regard to the rights of data subjects.	3. 본 규정을 적용 받는 개인정보처리자 또는 수탁처리자의 규정 준수와 더불어, 제3조에 따라 본 규정을 적용 받지 않는 개인정보처리자 또는 수탁처리자는 제46조(2) (e)호의 조건에 따라 제3국 또는 국제기구로의 개인정보 이전에 대한 프레임워크 안에서 적정한 안전조치를 제공하기 위해 본 조 제5항에 따라 승인된 행동강령과 본 조 제9항에 따라 일반적인 효력을 가지는 행동강령을 준수할 수 있다. 해당 개인정보처리자 또는 수탁처리자는 계약 증서 또는 기타의 법적 구속력이 있는 장치를 통해, 개인정보주체의 권리에 관해서 등 상기의 적정한 안전조치를 적용하기 위해 구속력 있고 강제할 수 있는 약속을 해야 한다.
4. A code of conduct referred to in paragraph 2 of this Article shall contain mechanisms which enable the body referred to in Article 41(1) to carry out the mandatory monitoring of compliance with its provisions by the controllers or processors which undertake to apply it, without prejudice to the tasks and powers of supervisory authorities competent pursuant to Article 55 or 56.	4. 본 조 제2항의 행동강령은 제41조(1)에 규정된 기관이 제55조와 제56조에 따른 감독기관의 업무와 권한을 침해하지 않고, 행동강령을 적용하기로 약속한 개인정보처리자와 수탁처리자가 해당 조문을 준수하는 것을 의무적으로 모니터링 할 수 있도록 하는 메커니즘을 포함해야 한다.

5. Associations and other bodies referred to in paragraph 2 of this Article which intend to prepare a code of conduct or to amend or extend an existing code shall submit the draft code, amendment or extension to the supervisory authority which is competent pursuant to Article 55. The supervisory authority shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation and shall approve that draft code, amendment or extension if it finds that it provides sufficient appropriate safeguards.	5. 행동강령을 작성하거나 기존 강령을 개정 또는 확대할 의도인 본 조 제2항의 협회 또는 기타 기관은 제55조에 따른 권한을 가지는 감독기관에 강령 초안이나 개정 또는 확대 강령을 제출해야 한다. 감독기관은 강령 초안이나 개정 또는 확대 강령이 본 규정에 부합하는지 여부에 대한 의견을 제시하고 적정한 안전조치를 제공한다고 판단되는 경우, 해당 초안이나 개정 또는 확대 강령을 승인해야 한다.
6. Where the draft code, or amendment or extension is approved in accordance with paragraph 5, and where the code of conduct concerned does not relate to processing activities in several Member States, the supervisory authority shall register and publish the code.	6. 강령 초안이나 개정 또는 확대 강령이 제5항에 따라 승인되는 경우, 또한 해당 행동 강령이 복수 회원국에서의 처리 활동과 관련되지 않을 경우, 감독기관은 그 강령을 등록 및 공개해야 한다.
7. Where a draft code of conduct relates to processing activities in several Member States, the supervisory authority which is competent pursuant to Article 55 shall, before approving the draft code, amendment or extension, submit it in the procedure referred to in Article 63 to the Board which shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation or, in the situation referred to in paragraph 3, provides appropriate safeguards.	7. 행동강령 초안이 복수 회원국에서의 처리 활동에 관련될 경우, 제55조에 따른 권한을 가지는 감독기관은 강령 초안이나 개정 또는 확대 강령을 승인하기 전에 제63조에 규정된 절차에 따라 유럽정보보호이사회에 이를 제출해야 하며, 이사회는 강령 초안이나 개정 또는 확대 강령이 본 규정을 준수하는지 여부, 또는 제3항에 규정된 상황에서, 적정한 안전조치를 제공하는지 여부에 대한 의견을 제시해야 한다.
8. Where the opinion referred to in paragraph 7 confirms that the draft code, amendment or extension complies with this Regulation, or, in the situation referred to in paragraph 3, provides appropriate safeguards, the Board shall submit its opinion to the Commission.	8. 제7항에 명시된 의견이 해당 강령 초안이나 개정 또는 확대 강령이 본 규정을 준수한다고 확정하거나 제3항에 규정된 상황에서 적정한 안전조치를 제공한다고 확정하는 경우, 유럽정보보호이사회는 본 의견을 집행위원회에 제출해야 한다.
9. The Commission may, by way of implementing acts, decide that the approved code of conduct, amendment or extension submitted to it pursuant to paragraph 8 have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).	9. 집행위원회는 이행 법률을 통해 제8항에 따라 제출된 승인된 행동강령이나 개정 또는 확대 강령이 유럽연합 내 일반적인 효력을 가진다고 결정할 수 있다. 그 이행 법률은 제93조(2)에 규정된 심사 절차에 따라 채택되어야 한다.
10. The Commission shall ensure appropriate publicity for the approved codes which have been decided as having general validity in accordance with paragraph 9.	10. 집행위원회는 제9항에 따라 일반적 효력을 가진다고 결정이 내려진 승인된 강령이 적절히 홍보되도록 해야 한다.
11. The Board shall collate all approved codes of conduct, amendments and extensions in a register and shall make them publicly available by way of appropriate means.	11. 유럽정보보호이사회는 승인된 행동강령과 개정 또는 확대된 강령 일체를 등록부에 취합하고 적절한 수단을 통해 이를 공개해야 한다.

Article 41 Monitoring of approved codes of conduct	제41조 승인된 행동강령의 모니터링
1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, the monitoring of compliance with a code of conduct pursuant to Article 40 may be carried out by a body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for that purpose by the competent supervisory authority.	1. 제57조와 제58조에 따른 관련 감독기관의 업무와 권한을 침해하지 않으면서, 제40조에 따른 행동강령의 준수에 대한 모니터링은 행동강령의 주제와 관련하여 적정 수준의 전문지식을 보유하고, 관련 감독기관이 그 목적으로 승인한 기관이 실시할 수 있다.
2. A body as referred to in paragraph 1 may be accredited to monitor compliance with a code of conduct where that body has: (a) demonstrated its independence and expertise in relation to the subject-matter of the code to the satisfaction of the competent supervisory authority; (b) established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation; (c) established procedures and structures to handle complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make those procedures and structures transparent to data subjects and the public; and (d) demonstrated to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.	2. 제1항의 기관은 다음 각 호에 해당하는 경우 행동강령의 준수를 모니터링하도록 승인받을 수 있다. (a) 감독기관이 만족할 수준의 독립성 및 강령의 주제와 관련한 전문지식을 입증한 경우 (b) 강령을 적용하는 개인정보처리자 및 수탁처리자의 적격성을 평가하고 관련 조문의 준수를 모니터링하며 강령의 이행을 정기적으로 검토할 수 있도록 하는 절차를 수립한 경우 (c) 강령 위반 및 개인정보처리자나 수탁처리자가 강령을 이행하였거나 이행하는 방식에 관한 민원을 처리하는 절차 및 구조를 수립하고, 그 절차와 구조를 개인정보주체와 일반에 투명하게 할 절차 및 구조를 수립한 경우 (d) 그 업무와 직무가 이해의 상충을 초래하지 않는다는 사실을 관련 감독기관이 만족할 정도로 입증하는 경우.
3. The competent supervisory authority shall submit the draft criteria for accreditation of a body as referred to in paragraph 1 of this Article to the Board pursuant to the consistency mechanism referred to in Article 63.	3. 관련 감독기관은 제63조의 일관성 메커니즘에 따라, 본 조 1항에 규정된 기관을 인증하기 위한 기준의 초안을 유럽정보보호이사회에 제출해야 한다.
4. Without prejudice to the tasks and powers of the competent supervisory authority and the provisions of Chapter VIII, a body as referred to in paragraph 1 shall, subject to appropriate safeguards, take appropriate action in cases of infringement of the code by a controller or processor, including suspension or exclusion of the controller or processor concerned from the code. It shall inform the competent supervisory authority of such actions and the reasons for taking them.	4. 관련 감독기관의 업무와 권한 및 제VIII장의 조문을 침해하지 않고, 제1항에 규정된 기관은 개인정보처리자 또는 수탁처리자가 강령을 위반하는 경우 적정한 안전조치에 따라 강령 이행의 중지나 배제 등의 적절한 조치를 취해야 한다. 해당 기관은 해당 조치와 해당 조치 사유를 감독기관에 통지해야 한다.
5. The competent supervisory authority shall revoke the accreditation of a body as referred to in paragraph 1 if the conditions for accreditation are not, or are no longer, met or where actions taken by the body infringe this Regulation.	5. 인증 조건이 충족되지 않거나 더 이상 충족되지 않는 경우 또는 제1항의 기관이 취한 조치가 본 규정을 위반하는 경우 관련 감독기관은 그 기관의 인증을 철회해야 한다.

6. This Article shall not apply to processing carried out by public authorities and bodies.	6. 본 조문은 공공기관 및 기타 기관이 시행하는 처리에는 적용되지 않는다.
Article 42 **Certification**	**제42조** **인증**
1. The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account.	1. 회원국과 감독기관, 유럽정보호이사회, 집행위원회는 개인정보처리자가 시행하는 처리 작업이 본 규정을 준수하고 있음을 입증하기 위한 목적으로 특히 유럽연합의 차원의 개인정보보호 인증 메커니즘, 개인정보보호 인장 및 마크의 수립을 장려해야 한다. 영세기업이나 중소기업의 특정 요구도 참작되어야 한다.
2. In addition to adherence by controllers or processors subject to this Regulation, data protection certification mechanisms, seals or marks approved pursuant to paragraph 5 of this Article may be established for the purpose of demonstrating the existence of appropriate safeguards provided by controllers or processors that are not subject to this Regulation pursuant to Article 3 within the framework of personal data transfers to third countries or international organisations under the terms referred to in point (f) of Article 46(2). Such controllers or processors shall make binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards, including with regard to the rights of data subjects.	2. 본 규정을 적용받는 개인정보처리자 또는 수탁처리자의 규정 준수와 더불어, 제46조(2) (f)호의 조건에 따른 제3국 또는 국제기구로의 개인정보 이전이라는 프레임워크 내에서 제3조에 의거 본 규정을 적용받지 않는 개인정보처리자 또는 수탁처리자가 제공하는 적정한 안전조치의 존재를 입증할 목적으로 본 조 제5항에 따라 승인된 개인정보 보호 인증 메커니즘, 인장 또는 마크가 수립될 수 있다. 해당 개인정보처리자나 수탁처리자는 개인정보주체의 권리와 관련해서 등, 상기의 적정한 안전조치를 적용하기 위해 계약적 또는 기타 구속력 있는 장치를 통해 구속력 및 강제력 있는 약속을 해야 한다.
3. The certification shall be voluntary and available via a process that is transparent.	3. 인증은 자발적이어야 하고 투명한 절차를 통해 제공되어야 한다.
4. A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the tasks and powers of the supervisory authorities which are competent pursuant to Article 55 or 56.	4. 본 조문에 따른 인증이 본 규정을 준수해야 하는 개인정보처리자 또는 수탁처리자의 책임을 경감하지는 않으며, 제55조 또는 제56조에 따라 권한을 가지는 감독기관의 업무와 권한을 침해하지 않는다.
5. A certification pursuant to this Article shall be issued by the certification bodies referred to in Article 43 or by the competent supervisory authority, on the basis of criteria approved by that competent supervisory authority pursuant to Article 58(3) or by the Board pursuant to Article 63. Where the criteria are approved by the Board, this may result in a common certification, the European Data Protection Seal.	5. 본 조문에 따른 인증은 제58조(3)항에 따른 관련 감독기관이나 제63조에 따른 유럽정보보호이사회가 승인한 기준을 토대로, 제43조의 인증기관 또는 관련 감독기관이 발급할 수 있다. 해당 기준이 유럽정보보호이사회에 의해 승인되는 경우, 이는 공동 인증인 유럽 정보보호 인장(European Data Protection Seal)으로 이어질 수 있다.
6. The controller or processor which submits its processing to the certification mechanism shall provide the certification body referred to in Article 43, or where applicable, the competent supervisory authority, with all information and access to its processing activities which are necessary to conduct the	6. 인증 메커니즘에 처리(정보)를 제출하는 개인정보처리자나 수탁처리자는 제43조의 인증기관이나 해당하는 경우 관련 감독기관에 인증절차를 실시하는 데 필요한 정보 및 처리활동에 대한 접근 일체를 제공해야 한다.

certification procedure.

7. Certification shall be issued to a controller or processor for a maximum period of three years and may be renewed, under the same conditions, provided that the relevant requirements continue to be met. Certification shall be withdrawn, as applicable, by the certification bodies referred to in Article 43 or by the competent supervisory authority where the requirements for the certification are not or are no longer met.

7. 인증은 최대 3년간 개인정보처리자나 수탁처리자에게 발급되어야 하며 관련 요건이 계속적으로 충족되는 경우 동일한 조건에 따라 갱신될 수 있다. 제43조에 규정된 인증기관 또는 관련 감독기관은 인증 요건이 충족되지 않을 경우, 인증을 철회하여야 한다.

8. The Board shall collate all certification mechanisms and data protection seals and marks in a register and shall make them publicly available by any appropriate means.

8. 유럽정보보호이사회는 인증 메커니즘, 개인정보보호 인장 및 마크의 일체를 등록부에 취합하고 적절한 수단을 통해 공개하여야 한다.

Article 43
Certification bodies

제43조
인증 기관

1. Without prejudice to the tasks and powers of the competent supervisory authority under Articles 57 and 58, certification bodies which have an appropriate level of expertise in relation to data protection shall, after informing the supervisory authority in order to allow it to exercise its powers pursuant to point (h) of Article 58(2) where necessary, issue and renew certification. Member States shall ensure that those certification bodies are accredited by one or both of the following:

   (a) the supervisory authority which is competent pursuant to Article 55 or 56;

   (b) the national accreditation body named in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council1 in accordance with EN-ISO/IEC 17065/2012 and with the additional requirements established by the supervisory authority which is competent pursuant to Article 55 or 56.

1. 제57조 및 제58조에 따라 권한을 가지는 감독기관의 업무와 권한을 침해하지 않고 개인정보 보호와 관련하여 적정 수준의 전문지식을 보유한 인증기관은 필요한 경우 감독기관이 제58조(2) (h)호에 따른 권한을 행사할 수 있도록 감독기관에 통지한 후 인증을 발급 및 갱신하여야 한다. 회원국은 그러한 인증기관이 다음 각 호의 하나 또는 모두에 의해 인증받았음을 보장해야 한다.

   (a) 제55조나 제56조에 따라 권한을 가지는 감독기관

   (b) EN-ISO/IEC 17065/2012 및 제55조나 제56조에 따라 권한을 가지는 감독기관이 정한 추가 요건에 부합하고 유럽의회 및 이사회 규정 (EC) 765/2008에 따라 명명된 국가 인증기관

2. Certification bodies referred to in paragraph 1 shall be accredited in accordance with paragraph 1 only where they have:

   (a) demonstrated their independence and expertise in relation to the subject-matter of the certification to the satisfaction of the competent supervisory authority;

   (b) undertaken to respect the criteria referred to in Article 42(5) and approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63;

   (c) established procedures for the issuing, periodic review and withdrawal of data protection certification, seals and marks;

   (d) established procedures and structures to handle complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the controller or processor, and to make those

2. 제1항의 인증기관은 다음 각 호에 해당하는 경우에 한하여 제1항에 따라 인증 받을 수 있다.

   (a) 인증 주제에 대해 감독기관이 만족할 정도의 독립성과 전문지식을 입증한 경우

   (b) 제42조(5)에 규정되고 제55조 또는 제56조에 따라 권한을 가지는 감독기관 또는 제63조에 따라 유럽정보보호이사회가 승인한 기준을 준수하기로 약속한 경우

   (c) 개인정보 보호 인증, 인장 및 마크의 발행, 정기 심사 및 철회에 관한 절차를 수립한 경우

   (d) 인증 위반 및 개인정보처리자나 수탁처리자가 인증을 이행하였거나 이행하는 방식에 관한 민원을 처리하는 절차 및 구조를 수립하고, 그 절차와 구조를 개인정보주체와 일반에 투명하게 할 절차 및 구조를 수립한 경우

   (e) 본인의 업무와 직무가 이해의 상충을 초래하지 않는다는 사실을 관할 감독기관이 만족할 정도로 입증한 경우

procedures and structures transparent to data subjects and the public; and (e) demonstrated, to the satisfaction of the competent supervisory authority, that their tasks and duties do not result in a conflict of interests.	
3. The accreditation of certification bodies as referred to in paragraphs 1 and 2 shall take place on the basis of criteria approved by the supervisory authority which is competent pursuant to Article 55 or 56 or by the Board pursuant to Article 63. In the case of accreditation pursuant to point (b) of paragraph 1 of this Article, those requirements shall complement those envisaged in Regulation (EC) No 765/2008 and the technical rules that describe the methods and procedures of the certification bodies.	3. 제1항 및 제2항의 인증기관의 인증은 제55조 또는 제56조에 따라 권한을 가지는 감독기관 또는 제63조에 따라 유럽정보보호이사회가 승인한 기준을 근거로 이루어져야 한다. 본 조 제1항 (b)호에 따른 인증의 경우, 본 요건은 규정(EC) 765/2008에서 예상되는 요건과 해당 인증기구의 방법과 절차를 기술하는 기술 규칙을 보완해야 한다.
4. The certification bodies referred to in paragraph 1 shall be responsible for the proper assessment leading to the certification or the withdrawal of such certification without prejudice to the responsibility of the controller or processor for compliance with this Regulation. The accreditation shall be issued for a maximum period of five years and may be renewed on the same conditions provided that the certification body meets the requirements set out in this Article.	4. 제1항의 인증기관은 개인정보처리자나 수탁처리자가 본 규정을 준수해야 할 책임을 침해하지 않고 인증 또는 그러한 인증의 철회를 초래하는 적절한 평가에 대한 책임을 져야 한다. 인증은 최대 5년의 기간 동안 발급되며 해당 인증기관이 본 조에 규정된 요건을 충족하는 경우에 한해 동일한 조건으로 갱신될 수 있다.
5. The certification bodies referred to in paragraph 1 shall provide the competent supervisory authorities with the reasons for granting or withdrawing the requested certification.	5. 제1항에 규정된 인증기관은 감독기관에 요청된 인증의 승인 또는 철회의 사유를 제공해야 한다.
6. The requirements referred to in paragraph 3 of this Article and the criteria referred to in Article 42(5) shall be made public by the supervisory authority in an easily accessible form. The supervisory authorities shall also transmit those requirements and criteria to the Board. The Board shall collate all certification mechanisms and data protection seals in a register and shall make them publicly available by any appropriate means.	6. 감독기관은 쉽게 이용할 수 있는 양식으로 본 조 제3항의 요건과 제42조(5)항의 기준을 공개해야 한다. 아울러 감독기관은 유럽정보보호이사회에 해당 요건과 기준을 전송해야 한다. 유럽정보보호이사회는 인증 메커니즘과 개인정보 보호 인장 일체를 등록부에 취합하고 적절한 수단을 통해 이를 공개해야 한다.
7. Without prejudice to Chapter VIII, the competent supervisory authority or the national accreditation body shall revoke an accreditation of a certification body pursuant to paragraph 1 of this Article where the conditions for the accreditation are not, or are no longer, met or where actions taken by a certification body infringe this Regulation.	7. 인증 조건이 충족되지 않거나 더 이상 충족되지 않는 경우, 또는 인증기관이 취한 조치가 본 규정을 위반하는 경우, 관련 감독기관이나 국가 인증기관은 제VIII장의 규정을 침해하지 않고 제1항의 인증기관의 인증을 철회해야 한다.
8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of specifying the requirements to be taken into account for the data protection certification mechanisms referred to in Article 42(1).	8. 집행위원회는 제42조(1)항에 규정된 개인정보 보호 인증 메커니즘에 고려되어야 할 요건을 규정할 목적으로 제92조에 따라 위임 법률을 채택할 권한이 있다.
9. The Commission may adopt implementing acts laying down	9. 집행위원회는 인증 메커니즘과 개인정보 보호 인장과 마크에 대한 기술

technical standards for certification mechanisms and data protection seals and marks, and mechanisms to promote and recognise those certification mechanisms, seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).

적 기준과 이러한 인증 메커니즘을 홍보하고 인정하는 메커니즘을 규정하는 이행 법률을 채택할 수 있다. 해당 이행 법률은 제93조(2)에 규정된 심사 절차에 따라 채택되어야 한다.

CHAPTER V
TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

제V장
제3국 및 국제기구로의 개인정보 이전

Article 44
General principle for transfers

제44조
이전을 위한 통칙

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.

현재 처리 중이거나 제3국 또는 국제기구로의 이전 후에 처리될 예정인 개인정보는 해당 제3국이나 국제기구로부터 기타 제3국이나 국제기구로 개인정보가 이전되는 경우 등 본 규정의 나머지 조문에 따라 개인정보처리자와 수탁처리자가 본 장에 규정된 조건을 준수하는 경우에만 그 이전이 가능해야 한다. 본 장의 규정 일체는 본 규정을 통해 보증되는 개인의 보호 수준을 보장하기 위해 적용되어야 한다.

Article 45
Transfers on the basis of an adequacy decision

제45조
적정성 결정에 따른 이전

1. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

1. 제3국 또는 국제기구로의 개인정보 이전은 집행위원회가 제3국, 해당 제3국의 영토나 하나 이상의 지정 부문, 또는 국제기구가 적정한 보호수준을 보장한다고 결정한 경우 가능하다. 그러한 이전에는 어떤 특정한 승인이 요구되지 않는다.

2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:

   (a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or

2. 보호 수준의 적정성을 평가할 때 집행위원회는 다음의 요소를 특히 고려해야 한다.

   (a) 법치주의, 인권 및 기본적 자유의 존중, 공안, 국방, 국가보안 및 형법, 공공기관의 개인정보 이용을 다룬 전반적·분야별 관련 법률, 이 같은 법률, 개인정보 규칙, 전문성 규칙, 보안 조치의 시행(향후 기타 제3국 또는 국제기구로의 개인정보 이전을 위한 규칙도 포함하는 이 규칙은 해당 제3국 또는 국제기구에서 준수되는 것임), 사법적 판례, 유효하고 구속력 있는 정보주체의 권리, 개인정보를 침해당한 개인정보주체를 위한 유효한 행정적 및 사법적 구제책

   (b) 개인정보주체의 권리 행사의 지원과 권고 및 회원국 감독기관들과의 협력 등 개인정보 보호 규정의 준수를 보장하고 강요할 의무가 있

international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred; (b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and (c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.	는, 제3국에 소재하거나 국제기구에 적용되는 하나 이상의 독립적 감독기관의 유무 및 해당 기관의 효과적인 작동 여부 (c) 특히 개인정보의 보호와 관련하여, 제3국이나 국제기구가 체결한 국제 협정, 또는 법적 구속력 있는 조약이나 문서 및 다자간·지역적 기구에의 참여로 인해 주어진 기타 의무
3. The Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country, a territory or one or more specified sectors within a third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2 of this Article. The implementing act shall provide for a mechanism for a periodic review, at least every four years, which shall take into account all relevant developments in the third country or international organisation. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority or authorities referred to in point (b) of paragraph 2 of this Article. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 93(2).	3. 집행위원회는 보호 수준의 적정성 여부를 평가한 후 제3국, 해당 제3국의 영토나 하나 이상의 지정 부문, 또는 해당 국제기구가 본 조 2항의 의미 내에서 적정한 보호 수준을 보장하는지를 판단할 수 있다. 이행 법률은 최소한 4년마다의 정기적 검토를 위한 메커니즘을 규정해야 하고 검토에는 제3국이나 국제기구 내의 관련 추이사항 일체가 고려되어야 한다. 이행 법률은 영토 및 부문별 적용에 대한 규정을 명시하고, 적용이 가능한 경우 본 조 제2항 (b)호의 감독기관(들)에 대해 확인해야 한다. 이행 법률은 제93조(2)의 검토 절차에 따라 채택되어야 한다.
4. The Commission shall, on an ongoing basis, monitor developments in third countries and international organisations that could affect the functioning of decisions adopted pursuant to paragraph 3 of this Article and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC.	4. 집행위원회는 본 조 제3항에 준하여 채택된 결정 및 지침 95/46/EC의 제25조(6)항을 근거로 채택된 결정의 작동에 영향을 미칠 수 있는 제3국 및 국제기구 내의 추이사항을 지속적으로 모니터링 해야 한다.
5. The Commission shall, where available information reveals, in particular following the review referred to in paragraph 3 of this Article, that a third country, a territory or one or more specified sectors within a third country, or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2 of this Article, to the extent necessary, repeal, amend or suspend the decision referred to in paragraph 3 of this Article by means of implementing acts without retro-active effect. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2). On duly justified imperative grounds of urgency, the Commission shall adopt immediately applicable implementing	5. 집행위원회는 가용 정보를 통해, 특히 제3항에 명시된 검토 이후 제3국, 해당 제3국의 영토나 하나 이상의 지정 부문, 또는 국제기구가 제2항에서 의미하는 적정한 보호 수준을 더 이상 보장하지 않는다고 판단될 경우, 필요한 정도까지 소급효 없이 제3항의 결정을 철회, 수정, 또는 중지시킬 수 있다. 이행 법률은 제93조(2)의 검토 절차를 따라 채택되어야 한다. 충분히 타당하고 긴요한 시급성의 근거가 있는 경우, 제93조(3)의 절차에 따라 집행위원회는 즉시 적용 가능한 이행 법률을 채택하여야 한다.

acts in accordance with the procedure referred to in Article 93(3).	
6. The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the decision made pursuant to paragraph 5.	6. 집행위원회는 제5항에 의거하여 내린 결정을 초래한 상황을 시정할 목적으로 제3국이나 국제기구와 협의해야 한다.
7. A decision pursuant to paragraph 5 of this Article is without prejudice to transfers of personal data to the third country, a territory or one or more specified sectors within that third country, or the international organisation in question pursuant to Articles 46 to 49.	7. 제5항에 의거한 결정은 제46조부터 제49조까지에 따른 해당의 제3국, 제3국의 영토나 하나 이상의 지정 부문, 또는 국제기구로의 개인정보 이전을 침해하지 않는다.
8. The Commission shall publish in the Official Journal of the European Union and on its website a list of the third countries, territories and specified sectors within a third country and international organisations for which it has decided that an adequate level of protection is or is no longer ensured.	8. 집행위원회는 적정한 보호 수준이 보장되거나 또는 더 이상 보장되지 않는다고 판단된 제3국, 제3국의 영토와 지정 부문, 및 국제기구 목록을 유럽연합 관보 및 웹사이트에 게재해야 한다.
9. Decisions adopted by the Commission on the basis of Article 25(6) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by a Commission Decision adopted in accordance with paragraph 3 or 5 of this Article.	9. 지침 95/46/EC의 제25조(6)를 근거로 집행위원회가 채택하는 결정은 본 조 제3항 또는 제5항에 따라 채택되는 집행위원회 결정으로 수정, 대체, 폐지될 때까지 유효해야 한다.
Article 46 **Transfers subject to appropriate safeguards**	**제46조** **적정한 안전조치에 의한 이전**
1. In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.	1. 제45조(3)에 의거한 결정이 없을 경우, 개인정보처리자나 수탁처리자는 적정한 안전조치를 제공한 경우에 한하여, 개인정보주체가 행사할 수 있는 권리와 유효한 법적 구제책이 제공되는 조건으로 제3국 또는 국제기구에 개인정보를 이전할 수 있다.
2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by: (a) a legally binding and enforceable instrument between public authorities or bodies; (b) binding corporate rules in accordance with Article 47; (c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2); (d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2); (e) an approved code of conduct pursuant to Article 40	2. 제1항의 적정한 안전조치는 감독기관의 특별한 승인을 요하지 아니하고 다음 각 호에 의해 제공될 수 있다. (a) 공공당국 또는 기관 간에 법적 구속력이 있고 강제할 수 있는 장치 (b) 제47조에 따른 의무적 기업 규칙 (c) 제93조(2)의 검토 절차에 따라 집행위원회가 채택한 정보보호 표준조항 (d) 감독기관이 채택하고 제93(2)조의 검토 절차에 따라 집행위원회가 승인한 정보보호 표준조항 (e) 개인정보주체의 권리에 관한 것 등 적정한 안전조치를 적용하기 위한 것으로 법적 구속력 및 강제력이 있는 제3국의 개인정보처리자나 수탁처리자의 약속을 포함한 제40조에 의거한 공인 행동강령 (f) 개인정보주체의 권리에 관한 것 등 적정한 안전조치를 적용하기 위

together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or (f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.	한 것으로 법적 구속력 및 강제력이 있는 제3국의 개인정보처리자나 수탁자처리자의 약속을 포함한 제42조에 의거한 공인 인증 메커니즘
3. Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by: (a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or (b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.	3. 제1항의 적정한 안전조치는 관할 감독기관의 승인을 거쳐 특히 다음 각 호를 통해서도 제공될 수 있다. (a) 개인정보처리자나 수탁처리자와 제3국이나 국제기구의 갸안정보처리자, 수탁처리자 또는 개인정보 수령인 간의 계약 조항 (b) 공공당국이나 기관 간의 행정 협정에 삽입될 것으로 강제력이 있고 유효한 개인정보주체의 권리를 포함한 규정
4. The supervisory authority shall apply the consistency mechanism referred to in Article 63 in the cases referred to in paragraph 3 of this Article.	4. 감독기관은 본 조 제3항의 사례의 경우 제63조의 일관성 메커니즘을 적용해야 한다.
5. Authorisations by a Member State or supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed, if necessary, by that supervisory authority. Decisions adopted by the Commission on the basis of Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed, if necessary, by a Commission Decision adopted in accordance with paragraph 2 of this Article.	5. 지침 95/46/EC의 제26조(2)를 근거로 한 회원국이나 감독기관의 승인은 필요한 경우 해당 감독기관이 수정, 대체, 철회할 때까지 유효해야 한다. 지침 95/46/EC의 제26조(4)를 근거로 집행위원회가 채택하는 결정은 필요한 경우 본 조 제2항에 따라 채택된 집행위원회 결정에 의해 수정, 대체 또는 철회될 때까지 유효해야 한다.
Article 47 **Binding corporate rules**	**제47조** **무적 기업 규칙**
1. The competent supervisory authority shall approve binding corporate rules in accordance with the consistency mechanism set out in Article 63, provided that they: (a) are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees; (b) expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and (c) fulfil the requirements laid down in paragraph 2.	1. 관할 감독기관은 제63조에 명시된 일관성 메커니즘에 따라 의무적 기업 규칙을 승인해야 한다. 단, 그 규칙이 다음 각 호를 전제로 해야 한다. (a) 법적 구속력이 있으며 피고용인 등 공동 경제활동에 관여하는 사업체 집단 또는 기업 집단의 모든 구성원들에게 적용되고 그들에 의해 이행되는 경우 (b) 본인의 개인정보 처리와 관련하여 개인정보주체에게 명시적으로 구속력 있는 권리를 부여하는 경우 (c) 제2항의 요건을 충족시키는 경우
2. The binding corporate rules referred to in paragraph 1 shall	2. 제1항의 의무적 기업 규칙은 최소한 다음 각 호를 명시해야 한다.

specify at least:

(a) the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;

(b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;

(c) their legally binding nature, both internally and externally;

(d) the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;

(e) the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with Article 22, the right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States in accordance with Article 79, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;

(f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union; the controller or the processor shall be exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage;

(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in addition to Articles 13 and 14;

(h) the tasks of any data protection officer designated in accordance with Article 37 or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling;

(i) the complaint procedures;

(j) the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred under point (h) and to the board of the controlling undertaking of a group of undertakings, or of the group of enterprises engaged in a joint economic

(a) 공동 경제활동에 관여하는 사업체 집단이나 기업 집단 및 각 구성원의 구조와 연락처

(b) 개인정보의 범주, 처리 유형과 목적, 관련 개인정보주체의 유형 및 해당 제3국의 신원 확인 등의 정보 이전 또는 이전 건 일체

(c) 내외부적으로 법적 구속력이 있는 특성

(d) 특히 목적제한과 데이터 최소화, 보관기간 제한, 정보 품질, 설계 및 기본설정에 의한 정보보호, 정보처리의 법적 근거, 특정 범주의 개인정보 처리, 정보 보안 확보 대책 등의 일반 정보보호 원칙 및 향후 의무적 기업 규칙의 구속을 받지 않는 기관에 대한 재이전과 관련된 요건의 적용

(e) 제22조에 의거한 프로파일링 등 자동 처리만을 근거로 한 결정을 따르지 않을 권리, 제79조에 의거한 관할 감독기관 및 회원국 관할 법원에 민원을 제기할 권리 그리고 구제 및 해당하는 경우 의무적 기업 규칙 위반에 대한 보상을 받을 권리 등 개인정보 처리에 관한 개인정보주체의 권리 및 이 권리를 행사하기 위한 수단

(f) 회원국 영토에 설립된 개인정보처리자 또는 수탁처리자가 유럽연합 역내에 설립되지 않은 구성원의 의무적 기업 규칙 위반에 대한 책임을 인정. 개인정보처리자 또는 수탁처리자는 해당 구성원이 피해를 초래한 사건에 대한 책임이 없음을 입증하는 경우에 한해 전적 또는 부분적으로 그 책임을 면제받아야 한다.

(g) 제13조 및 제14조에 더하여, 특히 본 항의 (d), (e), (f)호에 명시된 규정 등 의무적 기업 규칙에 관한 정보가 개인정보주체에 제공되는 방식

(h) 제37조에 따라 지정된 개인정보보호 담당관, 또는 공동 경제활동에 종사하는 사업체 집단이나 기업 집단 내에서 의무적 기업 규칙의 준수 여부 모니터링, 모니터링 교육 및 원처리를 담당하는 제3자 또는 주체의 업무

(i) 민원 절차

(j) 공동 경제활동에 관여하는 사업체 집단 또는 기업 집단 내의 의무적 기업 규칙의 준수 여부를 검증하기 위한 메커니즘. 그러한 메커니즘은 개인정보주체의 권리를 보호하기 위한 시정조치를 보장할 정보보호 감사 및 방법을 포함해야 한다. 해당 검증 결과는 (h)호의 개인이나 개체 및 기업 집단이나 그 사업을 총괄하는 이사회에게 통지해야 하고, 요청 시 관할 감독기관에 제공되어야 한다.

(k) 규칙의 변경사항을 보고 및 기록하기 위한 메커니즘과 해당 변경사항을 감독기관에 보고하기 위한 메커니즘

(l) 특히 (j)호의 조치 검증 결과를 감독기관에 공개함으로써 공동 경제활동에 종사하는 사업체 집단 또는 사업체 집단 구성원의 규칙 준수를 보장하기 위한 감독기관과의 협력 메커니즘

(m) 공동 경제활동에 종사하는 사업체 집단이나 기업 집단의 구성원이 제3국에서 적용을 받고, 의무적 기업 규칙이 보장하는 바에 상당한 악영향을 미칠 것으로 예상되는 법적 요건을 관할 감독기관에 보고하는 메커니즘

(n) 상시적 또는 정기적으로 개인정보를 열람할 수 있는 직원을 대상으로 한 적절한 정보보호 교육

activity, and should be available upon request to the competent supervisory authority;

(k) the mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority;

(l) the cooperation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority the results of verifications of the measures referred to in point (j);

(m) the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and

(n) the appropriate data protection training to personnel having permanent or regular access to personal data.

3. The Commission may specify the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).

3. 집행위원회는 본 조의 의미 내에서 의무적 기업 규칙에 대해 개인정보처리자, 수탁처리자, 감독기관 간에 이루어지는 정보 교환에 필요한 양식과 절차를 정할 수 있다. 그러한 이행 법률은 제93조(2)의 검토 절차에 따라 채택되어야 한다.

Article 48
Transfers or disclosures not authorised by Union law

제48조
유럽연합 법률로 승인되지 않은 정보의 이전 또는 제공

Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.

개인정보처리자나 수탁처리자가 개인정보를 이전하거나 제공하도록 요구하는 제3국의 법원이나 재판소의 판결 또는 행정기관의 결정은, 본 장에 의거한 기타 이전의 근거를 침해하지 않고, 요구한 제3국과 유럽연합이나 회원국 간에 유효한 상호 법률지원 조약 등의 국제협정을 기반으로 하는 경우 어떠한 방식으로도 인정되거나 강제될 수 있다.

Article 49
Derogations for specific situations

제49조
특정 상황에 대한 적용의 일부 제외

1. In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

(a) the data subject has explicitly consented to the proposed

1. 제4조 제3항의 적정성 결정이나 의무적 기업 규칙 등 제46조에 따른 적정한 안전조치가 없는 경우, 제3국이나 국제기구로의 개인정보 이전은 다음 각 호의 조건에 따라서만 가능하다.

(a) 적정성 결정 및 적절한 안전조치가 없음으로 인해 그 같은 개인정보의 이전이 개인정보주체에 초래할 수 있는 위험을 고지 받은 후 개인정보주체가 명시적으로 이전에 동의한 경우

transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

(d) the transfer is necessary for important reasons of public interest;

(e) the transfer is necessary for the establishment, exercise or defence of legal claims;

(f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case.

Where a transfer could not be based on a provision in Articles 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation pursuant to points (a) to (g) of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.

(b) 개인정보주체와 개인정보처리자 간의 계약을 이행하기 위해서나 개인정보주체의 요청으로 취한 계약 사전 조치를 이행하는 데 이전이 필요한 경우

(c) 개인정보주체의 이익을 위해 개인정보처리자와 기타 자연인 또는 법인 간에 체결된 계약의 이행을 위해 이전이 필요한 경우

(d) 중요한 공익상의 이유로 정보이전이 필요한 경우

(e) 법적 권리의 확립, 행사, 방어를 위해 정보이전이 필요한 경우

(f) 개인정보주체가 물리적 또는 법률적으로 동의를 할 수 없는 경우, 개인정보주체 또는 타인의 생명과 관련한 주요 이익을 보호하기 위해 정보이전이 필요한 경우

(g) 개인정보가 유럽연합 또는 회원국 법률에 따라 정보를 공개할 목적이거나 일반 국민 또는 정당한 이익을 입증할 수 있는 제3자가 참조(조회)하기 위한 목적으로 만들어진 개인정보 기록부(register)로부터 유럽연합 또는 회원국 법률에 명시된 참조(조회)의 조건이 충족되는 범위 내에서 이전되는 경우

정보의 이전이 의무적 기업 규칙에 대한 규정 등 제45조나 제46조의 규정을 근거로 할 수 없고, 본 항 (a)-(g)호에 따른 특정 상황에서의 일부 제외가 적용되지 않는 경우, 정보이전이 반복적이지 않고, 한정된 숫자의 정보주체에만 적용되고 개인정보주체의 이익이나 권리 및 자유가 우선하지 않는 한 개인정보처리자의 정당한 이익의 목적에 필요하며, 개인정보처리자가 정보이전과 관련한 일체의 정황을 평가한 후 그 결과를 토대로 개인정보 보호에 적절한 안전조치를 제시하는 경우에만 제3국이나 국제기구로의 정보이전이 가능하다. 개인정보처리자는 정보이전 사실을 감독기관에 고지해야 한다. 제13조 및 제14조에 명시된 정보 제공 이외에도 개인정보처리자는 해당 이전 및 본인의 설득력 있는 정당한 이익에 관한 정보를 정보주체에 고지해야 한다.

2. A transfer pursuant to point (g) of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

2. 제1항 (g)호에 따른 정보이전은 개인정보 기록부에 포함된 개인정보의 전부 또는 전체 범주와 관련되어서는 안 된다. 개인정보 기록부가 정당한 이익을 가진 자를 위한 참조(조회)의 목적으로 만들어진 경우, 정보의 이전은 해당인이 요청하는 경우 또는 이들이 수령인인 경우에만 가능해야 한다.

3. Points (a), (b) and (c) of the first subparagraph and the second subparagraph of paragraph 1 shall not apply to activities carried out by public authorities in the exercise of their public

3. 제1항 첫 단락의 (a), (b), (c)호 및 두 번째 단락은 공공기관이 공권력을 행사하여 시행하는 업무에는 적용되어서는 안 된다.

powers.	
4. The public interest referred to in point (d) of paragraph 1 shall be recognised in Union law or in the law of the Member State to which the controller is subject.	4. 제1항 (d)호의 공익은 개인정보처리자가 적용받는 유럽연합 또는 회원국 법률에서 인정되어야 한다.
5. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation. Member States shall notify such provisions to the Commission.	5. 적정성 결정이 없을 경우, 유럽연합 또는 회원국 법률은 중요한 공익상의 이유로 특정 범주의 개인정보를 제3국이나 국제기구로 전송하는 것을 명시적으로 제한할 수 있다. 회원국들은 해당 규정을 집행위원회에 통보해야 한다.
6. The controller or processor shall document the assessment as well as the suitable safeguards referred to in the second subparagraph of paragraph 1 of this Article in the records referred to in Article 30.	6. 개인정보처리자나 수탁처리자는 제30조의 기록부(records)에 본 조 제1항의 두 번째 단락에 명시된 평가 및 적절한 안전조치를 기록해야 한다.
Article 50 **International cooperation for the protection of personal data**	**제50조** **개인정보 보호를 위한 국제협력**
In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to: (a) develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data; (b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms; (c) engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data; (d) promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.	집행위원회와 감독기관은 제3국 및 국제기구와 관련하여 다음 각 호를 위한 적절한 조치를 시행해야 한다. (a) 개인정보 보호를 위한 법률의 효과적인 집행을 위한 국제협력 메커니즘 개발 (b) 개인정보 및 기타 기본적 권리와 자유를 보호하기 위한 적정한 안전조치에 따라, 통지, 민원 이첩, 조사 지원 및 정보 교환을 통해서 등 개인정보 보호를 위한 법률 집행에 대한 국제 상호 지원 제공 (c) 개인정보 보호를 위한 법률 집행 과정에서 국제협력을 촉진시킬 목적으로 논의 및 활동에 이해 당사자들을 참여시킬 것 (d) 제3국과의 사법권 분쟁에 관한 것 등 개인정보 보호 법률 및 관행에 대한 교류 및 문서화를 촉진

CHAPTER VI INDEPENDENT SUPERVISORY AUTHORITIES	제VI장 독립적인 감독기관
SECTION 1 INDEPENDENT STATUS	제1절 독립적인 지위
Article 51 Supervisory authority	제51조 감독기관
1. Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union.	1. 각 회원국은 처리와 관련하여 개인의 기본권과 자유를 보호하고 유럽연합 역내에서 개인 정보의 자유로운 이전을 촉진하기 위하여, 본 규정의 적용에 대한 모니터링을 전담할 하나 이상의 독립적인 공공기관을 제공해야 한다.
2. Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union. For that purpose, the supervisory authorities shall cooperate with each other and the Commission in accordance with Chapter VII.	2. 각 감독기관은 유럽연합 전역에 걸친 본 규정의 일관적인 적용에 일조해야 한다. 감독기관은 이러한 목적으로 제VII장에 의거하여 상호 간에 협력하고 집행위원회와 공조해야 한다.
3. Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority which is to represent those authorities in the Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 63.	3. 하나의 회원국에서 복수의 감독기관이 만들어질 경우, 해당 회원국은 유럽정보보호이사회에서 해당 감독기관들을 대표할 감독기관을 지정하고 제63조에 규정된 일관성 메커니즘과 관련한 규정을 다른 기관이 준수하도록 보장하는 메커니즘을 수립해야 한다.
4. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to this Chapter, by … [two years from the date of entry into force of this Regulation] at the latest and, without delay, any subsequent amendment affecting them.	4. 각 회원국은 제VI장에 의거하여 채택한 자국 법률의 조항을 최소한 [본 규정의 발효일자로부터 2년까지] 집행위원회에 고지하며, 이에 영향을 미치는 후속 개정안은 지체 없이 고지해야 한다.
Article 52 Independence	제52조 독립성
1. Each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation.	1. 각 감독기관은 본 규정에 따른 직무를 수행하고 권한을 행사하는 과정에서 완전한 독립성을 가지고 활동해야 한다.
2. The member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.	2. 각 감독기관의 위원(들)은 본 규정에 따라 부여된 직무를 수행하고 권한을 행사하는 과정에서 외부의 직간접적인 영향을 받지 아니하고, 다른 어떤 이로부터의 지시를 구하거나 받지 아니한다.

3. Member or members of each supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.	3. 각 감독기관의 위원(들)은 본인의 직무와 양립되지 않은 모든 행동은 삼가며, 재임기간 동안 대가 여부를 불문하고 직무와 양립 가능하지 않은 직업에 종사해서는 안 된다.
4. Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board.	4. 각 회원국은 상호 지원, 협력 및 유럽정보보호이사회에의 참여 차원에서 수행되는 직무와 권한 등, 효과적인 직무 수행 및 권한 행사에 필요한 인력과 기술, 재원, 부지 및 인프라를 감독기관이 제공받을 수 있도록 보장해야 한다.
5. Each Member State shall ensure that each supervisory authority chooses and has its own staff which shall be subject to the exclusive direction of the member or members of the supervisory authority concerned.	5. 각 회원국은 각 감독기관이 본 감독기관의 구성원의 지시만을 따르는 자체 인력을 선정 및 보유하도록 보장해야 한다.
6. Each Member State shall ensure that each supervisory authority is subject to financial control which does not affect its independence and that it has separate, public annual budgets, which may be part of the overall state or national budget.	6. 각 회원국은 각 감독기관이 독립성에 영향이 미치지 않는 선에서 재정적 통제를 받으며 각 감독기관이 국가의 전체 예산의 일부가 될 수 있는 별도의 연간 공식예산을 보유할 수 있도록 보장해야 한다.
Article 53 **General conditions for the members of the supervisory authority**	**제53조** **감독기관 위원(들)의 일반 조건**
1. Member States shall provide for each member of their supervisory authorities to be appointed by means of a transparent procedure by: - their parliament; - their government; - their head of State; or - an independent body entrusted with the appointment under Member State law.	1. 회원국은 감독기관의 각 위원이 다음의 투명한 절차를 통해 임명되도록 해야 한다. - 의회 - 정부 - 국가 수장 - 회원국 법률에 의해 임명이 위임된 독립적 기관
2. Each member shall have the qualifications, experience and skills, in particular in the area of the protection of personal data, required to perform its duties and exercise its powers.	2. 각 위원은 특히 개인정보 보호 분야에서, 각자의 직무를 수행하고 권한을 행사하는 데 필요한 자격과 경험 및 기량을 갖춰야 한다.
3. The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement, in accordance with the law of the Member State concerned.	3. 해당 회원국의 법률에 의거한 임기 만료, 사임, 또는 강제 해임 시 위원의 직무는 종료된다.

4. A member shall be dismissed only in cases of serious misconduct or if the member no longer fulfils the conditions required for the performance of the duties.	4. 위원은 중대한 위법행위가 있거나 직무 수행에 요구되는 조건을 더 이상 충족시키지 못하는 경우, 해임되어야 한다.
Article 54 **Rules on the establishment of the supervisory authority**	**제54조** **감독기관 설립에 관한 규칙**
1. Each Member State shall provide by law for all of the following: (a) the establishment of each supervisory authority; (b) the qualifications and eligibility conditions required to be appointed as member of each supervisory authority; (c) the rules and procedures for the appointment of the member or members of each supervisory authority; (d) the duration of the term of the member or members of each supervisory authority of no less than four years, except for the first appointment after … [the date of entry into force of this Regulation], part of which may take place for a shorter period where that is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure; (e) whether and, if so, for how many terms the member or members of each supervisory authority is eligible for reappointment; (f) the conditions governing the obligations of the member or members and staff of each supervisory authority, prohibitions on actions, occupations and benefits incompatible therewith during and after the term of office and rules governing the cessation of employment.	1. 각 회원국은 다음을 법률로 규정한다. (a) 각 감독기관의 설립 (b) 각 감독기관의 위원으로 임명되는데 필요한 자격과 적격 조건 (c) 각 감독기관 위원(들)의 임명 규칙 및 절차 (d) 본 규제의 발효 후 첫 임명을 제외하고, 4년 이상의 각 감독기관의 위원(들)의 임기. 단, 시차를 둔 임명 절차를 활용하여 감독기관의 독립성을 보호하기 위해 필요할 경우, 임기 중 일부를 단축할 수 있다 (e) 각 감독기관 위원(들)의 재임명 가능여부 및 임기 연장의 횟수 (f) 각 감독기관의 임직원의 의무에 관한 조건, 임기 도중과 이후 그에 양립되지 않는 행위나 직업, 편익에 대한 금지, 고용 중단에 관한 규칙
2. The member or members and the staff of each supervisory authority shall, in accordance with Union or Member State law, be subject to a duty of professional secrecy both during and after their term of office, with regard to any confidential information which has come to their knowledge in the course of the performance of their tasks or exercise of their powers. During their term of office, that duty of professional secrecy shall in particular apply to reporting by natural persons of infringements of this Regulation.	2. 각 감독기관의 임직원은 유럽연합 또는 회원국 법률에 따라 직무 수행 중 또는 권한 행사 과정에서 알게 된 기밀 정보와 관련하여 임기 중과 임기 후 직무상 기밀유지의 의무가 있다. 임기 중에 직업상 기밀유지의 임무는 특히 본 규정의 침해에 대한 개인의 신고에 적용 가능하다.
SECTION 2 **COMPETENCE, TASKS AND POWERS**	**제2절** **법적 자격, 업무 및 권한**
Article 55 **Competence**	**제55조** **법적 자격(competence)**
1. Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on	1. 각 감독기관은 본 규제에 의거하여 자체 회원국 영토에서 부여된 임무를 수행하고 권한을 행사하기 위한 법적 자격을 지닌다.

the territory of its own Member State.	
2. Where processing is carried out by public authorities or private bodies acting on the basis of points (c) or (e) of Article 6(1), the supervisory authority of the Member State concerned shall be competent. In such cases Article 56 does not apply.	2. 제6조(1)의 (c) 또는 (e)호를 근거로 활동하는 공공기관이나 민간기관에 의해 처리가 수행되는 경우, 해당 회원국의 감독기관은 이에 대한 법적 자격을 갖는다. 이 경우 제56조는 적용되지 아니한다.
3. Supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity.	3. 감독기관은 사법능력을 행사하는 법원의 처리방식을 감독할 법적 자격은 없다.
Article 56 **Competence of the lead supervisory authority**	**제56조** **선임 감독기관의 법적 자격**
1. Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.	1. 개인정보처리자 또는 수탁처리자의 주 사업장이나 단일 사업장의 감독기구는, 제55조를 침해하지 않으면서, 제60조에 규정된 절차에 따라 개인정보처리자 또는 수탁처리자가 수행하는 회원국 간의 처리에 대해 선임 감독기관으로 행동할 법적 자격을 지닌다.
2. By derogation from paragraph 1, each supervisory authority shall be competent to handle a complaint lodged with it or a possible infringement of this Regulation, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State.	2. 제1항의 적용이 일부 제외되어, 각 감독기관은 본 규정에 대한 위반에 관한 민원을 해결하거나 본 규정의 위반 가능성을 해결하는 법적 자격을 갖는다. 이는 관련 주제가 해당 회원국의 하나의 사업장만이 관련 있거나 해당 회원국의 개인정보주체에만 중대한 영향을 미치는 경우에만 해당된다.
3. In the cases referred to in paragraph 2 of this Article, the supervisory authority shall inform the lead supervisory authority without delay on that matter. Within a period of three weeks after being informed the lead supervisory authority shall decide whether or not it will handle the case in accordance with the procedure provided in Article 60, taking into account whether or not there is an establishment of the controller or processor in the Member State of which the supervisory authority informed it.	3. 본 조 제2항에 규정된 상황의 경우, 해당 감독기관은 지체 없이 관련 사안에 대해 선임 감독기관에 통지해야 한다. 통지를 받은 후 3주 이내에, 선임 감독기관은 감독기관이 고지한 회원국의 개인정보처리자 또는 수탁처리자의 사업장의 존재 여부를 고려하여, 제60조에 규정된 절차에 따라, 해당 상황을 처리할 지 여부를 결정해야 한다.
4. Where the lead supervisory authority decides to handle the case, the procedure provided in Article 60 shall apply. The supervisory authority which informed the lead supervisory authority may submit to the lead supervisory authority a draft for a decision. The lead supervisory authority shall take utmost account of that draft when preparing the draft decision referred to in Article 60(3).	4. 선임 감독기관이 관련 상황을 처리하기로 결정할 경우, 제60조에 규정된 절차가 적용된다. 선임 감독기관에 통보한 감독기관은 선임 감독기관에 결정문의 초안을 제출한다. 선임 감독기관은 제60조(3)에 규정된 결정문 초안을 작성할 때, 해당 초안을 최대한 고려해야 한다.
5. Where the lead supervisory authority decides not to handle the case, the supervisory authority which informed the lead supervisory authority shall handle it according to Articles 61 and 62.	5. 선임 감독기관이 관련 상황을 처리하지 않기로 결정할 경우, 선임 감독기관에 통보한 감독 기관은 제61조와 제62조에 의거하여 해당 상황을 처리해야 한다.

6. The lead supervisory authority shall be the sole interlocutor of the controller or processor for the cross-border processing carried out by that controller or processor.

6. 선임 감독기관은 개인정보처리자나 수탁처리자가 수행하는 회원국 간의 처리에 대해 개인정보처리자 또는 수탁처리자의 유일한 교섭담당기관이다.

Article 57
Tasks

제57조
업무

1. Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:

(a) monitor and enforce the application of this Regulation;

(b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention;

(c) advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing;

(d) promote the awareness of controllers and processors of their obligations under this Regulation;

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

(f) handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;

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

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

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

(j) adopt standard contractual clauses referred to in Article 28(8) and point (d) of Article 46(2);

(k) establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 35(4);

1. 본 규정에 규정된 다른 업무에 영향을 미치지 아니하고, 각 감독기관은 담당 권역에서 다음 각 호를 수행한다.

(a) 본 규정의 적용에 대한 모니터링 및 집행

(b) 처리와 관련된 위험, 규칙, 안전조치 및 권리에 대한 대중의 인식제고와 이해촉진. 구체적으로 아동을 다루는 활동의 경우, 각별한 주의가 필요하다

(c) 회원국 법률, 국가 의회, 정부 및 기타 기구 및 기관에 따라, 처리와 관련한 개인의 권리 및 자유의 보호에 대한 법률 및 행정 조치에 대한 자문

(d) 본 규정 의거한 개인정보처리자 및 수탁처리자의 각자 의무에 대한 인식 제고

(e) 요청 시, 본 규정에 따른 본인의 권리의 행사와 관한 정보를 개인정보주체에게 제공하고, 적절한 경우, 이를 위해 기타 회원국 내 감독기관과 공조

(f) 개인정보주체나 기관, 단체 또는 협회가 제80조에 따라 제기하는 민원을 처리하고, 적절한 범위 내에서 민원의 내용을 조사하고, 합리적인 기간 내에 조사의 진행 상황 및 결과를 민원인에게 통지, 특히 추가 조사나 다른 감독기관과의 조율이 필요한 경우

(g) 본 규정의 적용 및 집행의 일관성을 보장하기 위해, 정보 공유 및 상호 지원의 제공 등, 기타 감독기관과의 공조

(h) 기타 감독기관이나 공공기관으로부터 수령한 정보 등을 근거로 본 규정의 적용에 대한 조사 실시

(i) 특히 정보통신기술 및 상업적 관행의 개발 과정에서 개인정보 보호에 영향을 미치는 범위에서 관련 전개(developments) 상황에 대한 모니터링

(j) 제28조(8)과 제46조(2)의 (d)호에 규정된 정보보호 표준계약조항(standard contractual clauses)의 채택

(k) 제35조(4)에 따라 개인정보보호 영향평가에 대한 요건과 관련한 목록 수립 및 유지

(l) 제36조(2)에 규정된 처리 작업에 관한 자문 제공

(m) 제40조에 의거한 행동강령 마련을 장려하고 의견을 제시하며, 제40조(5)에 따라 충분한 안전조치를 제공하는 행동강령을 승인

(n) 제42조(1)에 따른 개인정보 보호 인증 메커니즘과 개인정보 보호 인장 및 상표의 제정 장려 및 제42조(5)에 의거한 인증 기준을 승인

(o) 해당되는 경우, 제42조(7)에 따라 공표되는 인증에 대한 정기적 검토의 실시

(p) 제41조에 의거한 행동강령의 모니터링 기관 및 제43조에 의거한 인증기관의 인증에 대한 기준의 초안 마련 및 공표

(l) give advice on the processing operations referred to in Article 36(2); (m) encourage the drawing up of codes of conduct pursuant to Article 40 and provide an opinion and approve such codes of conduct which provide sufficient safeguards, pursuant to Article 40(5); (n) encourage the establishment of data protection certification mechanisms and of data protection seals and marks pursuant to Article 42(1), and approve the criteria of certification pursuant to Article 42(5); (o) where applicable, carry out a periodic review of certifications issued in accordance with Article 42(7); (p) draft and publish the criteria for accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43; (q) conduct the accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43; (r) authorise contractual clauses and provisions referred to in Article 46(3); (s) approve binding corporate rules pursuant to Article 47; (t) contribute to the activities of the Board; (u) keep internal records of infringements of this Regulation and of measures taken in accordance with Article 58(2); and (v) fulfil any other tasks related to the protection of personal data.	(q) 제41조에 의거한 행동강령의 모니터링 기관 및 제43조에 의거한 인증기관의 인증 시행 (r) 제46조(3)에 규정된 계약조항 및 조문에 대한 승인 (s) 제47조에 의거한 의무적 기업규칙에 대한 승인 (t) 유럽정보보호이사회의 활동에 기여 (u) 본 규정의 위반과 제58조(2)에 따라 취해지는 조치에 대한 내부적 기록 보관 (v) 개인정보 보호와 관련된 기타 업무 수행
2. Each supervisory authority shall facilitate the submission of complaints referred to in point (f) of paragraph 1, by measures such as a complaint submission form which may also be completed electronically, without excluding other means of communication.	2. 각 감독기관은 다른 통지 수단을 배제하지 않고, 전자 양식으로도 작성 가능한 민원 제출 양식 등의 조치로 제1항 (f)호에 규정된 민원의 제출을 용이하게 한다.
3. The performance of the tasks of each supervisory authority shall be free of charge for the data subject and, where applicable, for the data protection officer.	3. 각 감독기관의 업무 수행에 대한 비용은 개인정보주체의 경우 무료이며, 해당되는 경우, 개인정보보호 담당관도 무료이다.
4. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the supervisory authority may charge a reasonable fee based on administrative costs, or refuse to act on the request. The supervisory authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.	4. 특히 요청의 반복적인 성격으로, 요청이 명백하게 근거가 없거나 지나칠 경우, 해당 감독기관은 행정적 비용에 근거한 합리적인 비용을 청구할 수 있거나 해당 요청에 대한 응대를 거절할 수 있다. 해당 감독기관은 관련 요청이 명백하게 근거가 없거나 과도한 성격임을 입증할 책임을 지닌다.

Article 58 Powers	제58조 권한
1. Each supervisory authority shall have all of the following investigative powers: (a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks; (b) to carry out investigations in the form of data protection audits; (c) to carry out a review on certifications issued pursuant to Article 42(7); (d) to notify the controller or the processor of an alleged infringement of this Regulation; (e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks; (f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.	1. 각 감독기관은 아래의 조사 권한을 모두 보유한다. (a) 개인정보처리자와 수탁처리자 그리고 해당되는 경우, 개인정보처리자 또는 수탁처리자의 대리인에게 업무의 수행에 필요한 정보의 일체를 제공하도록 명령 (b) 개인정보보호 감사의 형식의 조사 실시 (c) 제42조(7)에 의거하여 발급된 인증에 대한 검토 실시 (d) 개인정보처리자 또는 수탁처리자에게 본 규정의 위반 혐의 사안의 통지 (e) 개인정보처리자 또는 수탁처리자로부터 업무 수행에 필요한 모든 개인정보 및 모든 정보에 대한 열람권 취득 (f) 유럽연합 또는 회원국의 절차 법률에 따라, 모든 개인정보 처리 장치 및 수단 등, 개인정보처리자와 수탁처리자의 영역에 대한 열람권 취득
2. Each supervisory authority shall have all of the following corrective powers: (a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation; (b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation; (c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation; (d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period; (e) to order the controller to communicate a personal data breach to the data subject; (f) to impose a temporary or definitive limitation including a ban on processing; (g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Articles 17(2) and 19;	2. 각 감독기관은 다음의 시정 권한을 모두 보유한다. (a) 예정된 처리작업(들)이 본 규정의 조문을 위반할 가능성이 높은 것에 대해 개인정보처리자 또는 수탁처리자에게 경고 발령 (b) 예정된 처리작업(들)이 본 규정의 조문을 위반한 경우, 개인정보처리자 및 수탁처리자를 견책 (c) 개인정보처리자 및 수탁처리자가 본 규정에 따라 본인의 권리를 행사하고자 하는 개인정보주체의 요청을 따를 것을 지시 (d) 개인정보처리자 또는 수탁처리자에게 처리작업(들)이 본 규정의 조문을 준수하도록 지시하며, 적절한 경우, 구체적인 방식과 구체적인 기간 내에 하도록 지시 (e) 개인정보주체에게 개인정보 침해에 대해 통지하도록 수탁처리자에게 지시 (f) 처리에 대한 금지 등, 임시 또는 확정적 제한 부과 (g) 제16조, 제17조, 제18조에 따른 처리의 수정이나 삭제 또는 제한을 지시하고, 제17조(2) 및 제19조에 따라 개인정보를 제공받는 수령인들에게 이러한 행동조치에 대한 통지를 지시 (h) 인증의 요건이 충족되지 않거나 더 이상 충족되지 않는 경우, 인증을 철회하거나 인증기관에게 제42조 및 제42조에 의거하여 발급된 인증을 철회하라고 지시하거나 인증기관에게 인증을 발급하지 않도록 지시 (i) 각 개별 상황별 정황에 따라 본 조항에 규정된 조치를 부과하거나, 이와 함께 또는 이것 대신, 제83조에 따른 행정적 벌금을 부과 (j) 제3국 또는 국제기구의 수령인으로의 정보 이동의 중지를 지시

(h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met; (i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case; (j) to order the suspension of data flows to a recipient in a third country or to an international organisation.	
3. Each supervisory authority shall have all of the following authorisation and advisory powers: (a) to advise the controller in accordance with the prior consultation procedure referred to in Article 36; (b) to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data; (c) to authorise processing referred to in Article 36(5), if the law of the Member State requires such prior authorisation; (d) to issue an opinion and approve draft codes of conduct pursuant to Article 40(5); (e) to accredit certification bodies pursuant to Article 43; (f) to issue certifications and approve criteria of certification in accordance with Article 42(5); (g) to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2); (h) to authorise contractual clauses referred to in point (a) of Article 46(3); (i) to authorise administrative arrangements referred to in point (b) of Article 46(3); (j) to approve binding corporate rules pursuant to Article 47.	3. 각 감독기관은 다음의 모든 승인 및 자문권한을 보유한다. (a) 제36조에 규정된 사전 자문의 절차에 따라 수탁처리자에게 자문을 제공 (b) 자체 재량이나 요구에 따라, 해당 국가의 국회, 회원국의 정부 또는 회원국 법률에 따라 기타 기구 및 기관과 일반에 개인정보 보호와 관련한 사안에 대한 의견을 제공 (c) 회원국 법률에서 사전 승인을 요구하는 경우, 제36조(5)에 규정된 처리에 대한 승인 (d) 제40조(5)에 따른 의견 제공 또는 행동강령의 초안에 대한 승인 (e) 제42조에 따른 인증기관의 인증 (f) 제42조(5)에 따른 인증 발급 또는 인증의 기준에 대한 승인 (g) 제28조(8) 및 제46조(2)에 규정된 정보보호 표준조항의 채택 (h) 제46조(3)의 (a)호에 규정된 정보보호 계약조항에 대한 승인 (i) 제46조(3)의 (b)호에 규정된 행정적 협약에 대한 승인 (j) 제47조에 따른 의무적 기업규칙에 대한 승인
4. The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union and Member State law in accordance with the Charter.	4. 본 조문에 따라 감독기관에게 수여된 권한의 행사는 헌장에 따른 유럽 연합 및 회원국 법률에 규정된 유효한 사법구제 및 정밀 실사 등, 적절한 안전조치를 적용 받는다.
5. Each Member State shall provide by law that its supervisory authority shall have the power to bring infringements of this Regulation to the attention of the judicial authorities and where appropriate, to commence or engage otherwise in legal proceedings, in order to enforce the provisions of this	5. 각 회원국은 감독기관이 본 규제의 위반 사례를 사법기관에 고발할 권한과, 적절한 경우 본 규정의 조문을 집행하기 위해, 그 외의 법적 절차를 시작하거나 관련시킬 수 있는 권한을 가지고 있음을 법률적으로 규정하고 있다.

Regulation.	
6. Each Member State may provide by law that its supervisory authority shall have additional powers to those referred to in paragraphs 1, 2 and 3. The exercise of those powers shall not impair the effective operation of Chapter VII.	6. 각 회원국은 자국의 감독기관이 제1항, 제2항 및 제3항에 규정된 권한 외 추가적인 권한을 보유하고 있음을 법률로 규정할 수 있다. 이러한 권한의 행사는 제VII장의 유효한 작업을 방해하지 않는다.
Article 59 **Activity reports**	**제59조** **활동 보고서**
Each supervisory authority shall draw up an annual report on its activities, which may include a list of types of infringement notified and types of measures taken in accordance with Article 58(2). Those reports shall be transmitted to the national parliament, the government and other authorities as designated by Member State law. They shall be made available to the public, to the Commission and to the Board.	각 감독기관은 신고된 위반사건의 유형과 제58조(2)에 따라 취해진 조치의 유형의 목록을 포함할 수 있는 관련 활동에 대한 연차보고서를 작성해야 한다. 해당 보고서는 해당 국가의 의회, 정부, 그리고 회원국 법률이 지정한 관련 기관에 전달되어야 한다. 해당 보고서는 대중, 집행위원회 및 유럽정보보호이사회에 공개되어야 한다.
CHAPTER VII **COOPERATION AND CONSISTENCY**	**제VII장** **협력 및 일관성**
SECTION 1 **COOPERATION**	**제1절** **협력**
Article 60 **Cooperation between the lead supervisory authority and other supervisory authorities concerned**	**제60조** **선임 감독기관과 기타 관련 감독기관 간 협력**
1. The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavour to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other.	1. 선임 감독기관은 합의 도출을 위한 노력으로 본 조문에 의거하여 나머지 관련 감독기관과 협조해야 한다. 선임 감독기관 및 관련 감독기관은 모든 관련 정보를 서로 교환해야 한다.
2. The lead supervisory authority may request at any time other supervisory authorities concerned to provide mutual assistance pursuant to Article 61 and may conduct joint operations pursuant to Article 62, in particular for carrying out investigations or for monitoring the implementation of a measure concerning a controller or processor established in another Member State.	2. 선임 감독기관은 제61조에 의거하여 언제든지 기타 관련 감독기관에게 상호지원을 요청할 수 있고, 특히 조사를 실시하거나 타 회원국에 설립된 개인정보처리자 또는 수탁처리자에 관한 조치의 이행을 모니터링 하기 위해 제62조에 따른 공동 작업을 시행할 수도 있다.
3. The lead supervisory authority shall, without delay, communicate the relevant information on the matter to the other supervisory authorities concerned. It shall without delay submit a draft decision to the other supervisory authorities	3. 선임 감독기관은 지체 없이 그 사안에 관한 정보를 나머지 관련 감독기관에게 전달해야 한다. 의견 수렴을 위해 지체 없이 결정(안)을 나머지 관련 감독기관에게 제출해야 하고 그들의 견해를 신중히 고려해야 한다.

concerned for their opinion and take due account of their views.	
4. Where any of the other supervisory authorities concerned within a period of four weeks after having been consulted in accordance with paragraph 3 of this Article, expresses a relevant and reasoned objection to the draft decision, the lead supervisory authority shall, if it does not follow the relevant and reasoned objection or is of the opinion it is not relevant and reasoned, submit the matter to the consistency mechanism referred to in Article 63.	4. 나머지 관련 감독기관이 본 조 제3항에 따라 자문을 받은 후 4주의 기간 내에 결정(안)에 대하여 적정하고 타당한 반대 의사를 표명할 경우, 선임 감독기관은 이와 같은 적정하고 타당한 반대 의견에 따르지 않거나 그것이 적정하고 타당하지 않다는 의견이 있을 경우, 제63조에서 규정된 일관성 메커니즘에 그 사안을 상정해야 한다.
5. Where the lead supervisory authority intends to follow the relevant and reasoned objection made, it shall submit to the other supervisory authorities concerned a revised draft decision for their opinion. That revised draft decision shall be subject to the procedure referred to in paragraph 4 within a period of two weeks.	5. 선임 감독기관이 해당의 적정하고 타당한 반대 의사를 따르고자 할 경우, 의견 수렴을 위해 수정한 결정(안)을 나머지 관련 감독기관에 제출해야 한다. 수정된 결정(안)은 2주의 기간 내에 제4항에 명시된 절차의 적용을 받는다.
6. Where none of the other supervisory authorities concerned has objected to the draft decision submitted by the lead supervisory authority within the period referred to in paragraphs 4 and 5, the lead supervisory authority and the supervisory authorities concerned shall be deemed to be in agreement with that draft decision and shall be bound by it.	6. 어느 관련 감독기관도 제4항 및 제5항에 명시된 기간 내에 선임 감독기관이 제출한 결정(안)에 반대 의사를 표명하지 않은 경우, 선임 감독기관 및 관련 감독기관은 해당 결정(안)에 합의한 것으로 간주되고 그것을 따라야 한다.
7. The lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller or processor, as the case may be and inform the other supervisory authorities concerned and the Board of the decision in question, including a summary of the relevant facts and grounds. The supervisory authority with which a complaint has been lodged shall inform the complainant on the decision.	7. 선임 감독기관은 해당 결정을 채택하고 개인정보처리자 또는 수탁처리자의 주 사업장이나 단일 사업장에 고지해야 하며, 경우에 따라 나머지 관련 감독기관 및 유럽정보보호이사회에도 관련 사실과 근거의 개요 등 해당 결정을 통보해야 한다. 민원을 접수한 감독기관은 민원인에게 결정에 대해 통보해야 한다.
8. By derogation from paragraph 7, where a complaint is dismissed or rejected, the supervisory authority with which the complaint was lodged shall adopt the decision and notify it to the complainant and shall inform the controller thereof.	8. 제7항 적용의 일부 제외로 인해 민원이 묵살 또는 거부되는 경우, 해당 민원을 접수한 감독기관은 결정을 채택하고 그 사실을 민원인과 해당 개인정보처리자에게 알려야 한다.
9. Where the lead supervisory authority and the supervisory authorities concerned agree to dismiss or reject parts of a complaint and to act on other parts of that complaint, a separate decision shall be adopted for each of those parts of the matter. The lead supervisory authority shall adopt the decision for the part concerning actions in relation to the controller, shall notify it to the main establishment or single establishment of the controller or processor on the territory of its Member State and shall inform the complainant thereof, while the supervisory authority of the complainant shall adopt the decision for the part concerning dismissal or rejection of that complaint, and shall notify it to that complainant and shall inform the controller or processor thereof.	9. 선임 감독기관 및 관련 감독기관이 민원의 일부를 묵살 또는 거부하고 해당 민원의 다른 부분에 대하여 조치를 취하기로 합의할 경우, 그 사안에 대한 각각의 부분마다 별도의 결정을 채택해야 한다. 선임 감독기관이 개인정보처리자와 관련한 조치에 관한 부분에 대해 결정을 채택하고, 자국 영토에 있는 개인정보처리자 또는 수탁처리자의 주 사업장이나 단일 사업장에 고지하며, 해당 민원인에게 통보해야 한다. 한편 민원을 접수한 감독기관은 해당 민원의 묵살 또는 거부와 관련한 부분에 대한 결정을 채택하고, 이를 해당 민원인에게 통보하며, 해당 개인정보처리자 또는 수탁처리자에 통보해야 한다.

10. After being notified of the decision of the lead supervisory authority pursuant to paragraphs7 and 9, the controller or processor shall take the necessary measures to ensure compliance with the decision as regards processing activities in the context of all its establishments in the Union. The controller or processor shall notify the measures taken for complying with the decision to the lead supervisory authority, which shall inform the other supervisory authorities concerned.	10. 제7항 및 제9항에 따라 선임 감독기관의 결정을 고지 받은 후, 개인정보처리자 또는 수탁처리자는 유럽연합 내 모든 사업장의 활동 중에 시행되는 정보처리에 대하여 그 결정을 준수하기 위해 필요한 조치를 취해야 한다. 개인정보처리자 또는 수탁처리자는 결정을 준수하기 위해 취한 조치를 선임 감독기관에게 고지하고, 선임 감독기관은 나머지 관련 감독기관에게 통보해야 한다.
11. Where, in exceptional circumstances, a supervisory authority concerned has reasons to consider that there is an urgent need to act in order to protect the interests of data subjects, the urgency procedure referred to in Article 66 shall apply.	11. 예외적인 상황에서 관련 감독기관이 개인정보주체의 이익을 보호하기 위해 시급히 조치를 취해야 할 필요가 있다고 판단할 근거가 있을 경우, 제66조에 명시된 시급성의 절차가 적용된다.
12. The lead supervisory authority and the other supervisory authorities concerned shall supply the information required under this Article to each other by electronic means, using a standardised format.	12. 선임 감독기관 및 나머지 관련 감독기관은 본 조문에 따라 요구되는 정보를 표준화된 형식을 사용하여 전자적 수단에 의해 상호 제공해야 한다.
Article 61 **Mutual assistance**	**제61조** **상호 지원**
1. Supervisory authorities shall provide each other with relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective cooperation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations.	1. 본 규정을 일관적으로 시행 및 적용하기 위해 감독기관들은 서로 관련 정보와 상호 지원을 제공하고, 상호 간의 효과적인 협력을 위한 조치를 구비해야 한다. 특히 상호 지원은 사전 승인과 협의, 검사 및 조사 실시 요청 등의 정보 요청 및 감독적 조치를 망라해야 한다.
2. Each supervisory authority shall take all appropriate measures required to reply to a request of another supervisory authority without undue delay and no later than one month after receiving the request. Such measures may include, in particular, the transmission of relevant information on the conduct of an investigation.	2. 각 감독기관은 부당한 지체 없이 요청 접수 후 늦어도 한 달 이내에 타 감독기관의 요청에 응답하기 위해 요구되는 모든 적정한 조치를 취해야 한다. 그 같은 조치에는 조사 실시에 관한 정보의 전송이 포함될 수 있다.
3. Requests for assistance shall contain all the necessary information, including the purpose of and reasons for the request. Information exchanged shall be used only for the purpose for which it was requested.	3. 지원 요청에는 요청의 목적과 요청 사유 등의 필요한 정보가 포함되어야 한다. 교환되는 정보는 당초 요청된 목적으로만 사용되어야 한다.
4. The requested supervisory authority shall not refuse to comply with the request unless: (a) it is not competent for the subject-matter of the request or for the measures it is requested to execute; or	4. 지원 요청을 받은 감독기관은 다음의 경우가 아닌 한 지원을 거절해서는 안 된다 (a) 요청 대상이나 이행 요청이 들어온 조치에 대하여 할 수 있는 것이 없거나

(b) compliance with the request would infringe this Regulation or Union or Member State law to which the supervisory authority receiving the request is subject.	(b) 요청에 응할 경우 본 규정 또는 요청을 접수한 감독기관이 적용 받는 유럽연합 또는 회원국 법률에 위배될 경우.
5. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress of the measures taken in order to respond to the request. The requested supervisory authority shall provide reasons for any refusal to comply with a requestpursuant to paragraph 4.	5. 요청을 받은 감독기관은 경우에 따라 요청에 응하기 위해 취한 조치의 결과 또는 진행 상황을 통지해야 한다. 요청을 받은 감독기관은 제4항에 따라 요청의 응대를 거부하는 사유를 제공해야 한다.
6. Requested supervisory authorities shall, as a rule, supply the information requested by other supervisory authorities by electronic means, using a standardised format.	6. 규정에 따라, 요청을 받은 감독기관은 타 감독기관이 요구한 정보를 표준화된 형식을 사용하여 전자적 수단으로 제공해야 한다.
7. Requested supervisory authorities shall not charge a fee for any action taken by them pursuant to a request for mutual assistance. Supervisory authorities may agree on rules to indemnify each other for specific expenditure arising from the provision of mutual assistance in exceptional circumstances.	7. 요청을 받은 감독기관은 상호 지원 요청에 의거하여 그들이 취한 조치에 대해 비용을 청구해서는 안 된다. 감독기관들은 예외적인 상황에서 상호 지원의 제공으로 야기되는 특정 지출에 대해 서로 보상하는 규정에 대해 합의할 수 있다.
8. Where a supervisory authority does not provide the information referred to in paragraph 5 within one month of receiving the request of another supervisory authority, the requesting supervisory authority may adopt a provisional measure on the territory of its Member State in accordance with Article 55(1). In that case, the urgent need to act under Article 66(1) shall be presumed to be met and require an urgent binding decision from the Board pursuant to Article 66(2).	8. 한 감독기관이 타 감독기관으로부터 요청을 접수한 후 한 달 이내에 제5항에 언급된 정보를 제공하지 않을 경우, 요청 감독기관은 제55(1)조에 의거하여 자국의 영토에서 잠정적 조치를 채택할 수 있다. 이 경우, 제66조(1)의 조치의 시급한 필요성이 충족된 것으로 간주되어야 하고 이로써 제66조(2)에 따라 유럽정보보호이사회로부터 구속력 있는 긴급한 결정이 요구된다.
9. The Commission may, by means of implementing acts, specify the format and procedures for mutual assistance referred to in this Article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board, in particular the standardised format referred to in paragraph 6 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).	9. 집행위원회는, 이행 법률을 통해, 본 조문에 명시된 상호 지원을 위한 형식과 절차 및 제6항에 명시된 표준 양식 등 감독기관들 간, 그리고 감독기관과 유럽정보보호이사회 간에 전자적 수단에 의한 정보 교환 방식을 규정할 수 있다. 이 같은 이행 법률은 제93조(2)에 명시된 검토절차에 따라 채택되어야 한다.
Article 62 **Joint operations of supervisory authorities**	**제62조** **감독기관의 공동 작업**
1. The supervisory authorities shall, where appropriate, conduct joint operations including joint investigations and joint enforcement measures in which members or staff from the supervisory authorities of other Member States are involved.	1. 감독기관은 적정한 경우 기타 회원국의 감독기관들이 관여하는 공동 조사 및 공동 이행 조치 등의 공동 작업을 수행해야 한다.
2. Where the controller or processor has establishments in several	2. 개인정보처리자 또는 수탁처리자가 여러 회원국에 사업장을 두고 있거

Member States or where a significant number of data subjects in more than one Member State are likely to be substantially affected by processing operations, a supervisory authority of each of those Member States shall have the right to participate in joint operations. The supervisory authority which is competent pursuant to Article 56 (1) or 56(4) shall invite the supervisory authority of each of those Member States to take part in the joint operations and shall respond without delay to the request of a supervisory authority to participate.	나 하나 이상의 회원국에서 상당수의 정보주체들이 정보처리에 의해 실질적인 영향을 받을 가능성이 있는 경우, 각 해당 회원국의 감독기관은 공동 작업에 참여할 권리를 가져야 한다. 제56조(1) 또는 제56조(4)에 따른 관할 감독기관은 각 회원국의 감독기관을 공동 작업에 참여시키고 감독기관의 참여 요청에 지체 없이 응답하여야 한다.
3. A supervisory authority may, in accordance with Member State law, and with the seconding supervisory authority's authorisation, confer powers, including investigative powers on the seconding supervisory authority's members or staff involved in joint operations or, in so far as the law of the Member State of the host supervisory authority permits, allow the seconding supervisory authority's members or staff to exercise their investigative powers in accordance with the law of the Member State of the seconding supervisory authority. Such investigative powers may be exercised only under the guidance and in the presence of members or staff of the host supervisory authority. The seconding supervisory authority's members or staff shall be subject to the Member State law of the host supervisory authority.	3. 감독기관은 회원국 법률에 따라 부속 감독기관(seconding supervisory authority)의 승인을 받아 조사권 등의 권한을 공동 작업에 관여하는 부속 감독기관의 위원 또는 직원들에게 부여하거나, 주최 감독기관(host supervisory authority)의 회원국 법률이 허용하는 한에 있어서 부속 감독기관의 위원 또는 직원들이 자국의 법률에 따라 조사권한을 행사하도록 할 수 있다. 그 같은 조사권한은 주최 감독기관의 위원이나 직원의 안내 및 참관 하에서만 행사될 수 있다. 부속 감독기관의 위원이나 직원들은 주최 감독기관의 회원국 법률의 적용을 받아야 한다.
4. Where, in accordance with paragraph 1, staff of a seconding supervisory authority operate in another Member State, the Member State of the host supervisory authority shall assume responsibility for their actions, including liability, for any damage caused by them during their operations, in accordance with the law of the Member State in whose territory they are operating.	4. 제1항에 의거하여, 부속 감독기관의 직원이 타 회원국에서 활동할 경우, 주최 감독기관의 회원국은 해당 기관이 운영되는 회원국의 법률에 따라 업무 중에 발생하는 피해에 대한 책임 등 기관의 활동에 대한 책임을 져야 한다.
5. The Member State in whose territory the damage was caused shall make good such damage under the conditions applicable to damage caused by its own staff. The Member State of the seconding supervisory authority whose staff has caused damage to any person in the territory of another Member State shall reimburse that other Member State in full any sums it has paid to the persons entitled on their behalf.	5. 피해가 발생한 회원국은 자국 직원이 초래한 피해에 적용되는 조건에 따라 피해를 보상해야 한다. 타 회원국의 영토에서 타인에게 피해를 유발한 직원이 소속된 부속 감독기관의 회원국은 상대 회원국이 피해를 입은 당사자에게 대신 지불한 피해액을 전액 변상해야 한다.
6. Without prejudice to the exercise of its rights vis-à-vis third parties and with the exception of paragraph 5, each Member State shall refrain, in the case provided for in paragraph 1, from requesting reimbursement from another Member State in relation to damage referred to in paragraph 4.	6. 제3자에 대한 권리 행사를 침해하지 않고 제5항을 예외로 하여, 각 회원국은 제1항에 규정된 사례의 경우 제4항에 명시된 피해와 관련하여 타 회원국으로부터의 배상 요구를 자제해야 한다.
7. Where a joint operation is intended and a supervisory authority does not, within one month, comply with the obligation laid down in the second sentence of paragraph 2 of this Article, the other supervisory authorities may adopt a provisional measure on the territory of its Member State in accordance with Article 55. In that case, the urgent need to act under Article 66(1) shall be presumed to be met and require an opinion or an urgent binding decision from the Board pursuant to Article	7. 공동 작업이 예정되어 있고 감독기관이 한 달 내에 제2항의 두 번째 문장에 규정된 의무를 준수하지 않는 경우, 나머지 감독기관들은 제55조에 따라 자국의 영토에서 잠정적 조치를 채택할 수 있다. 그 같은 경우, 제66조(1)에 규정된 조치의 시급한 필요성이 충족된다고 간주되어야 하고 이로써 제66조(2)에 따라 유럽정보보호이사회로부터 의견 또는 구속력 있는 긴급한 결정이 요구되어야 한다.

66(2).

SECTION 2
CONSISTENCY

제2절
일관성

Article 63
Consistency mechanism

제63조
일관성 메커니즘

In order to contribute to the consistent application of this Regulation throughout the Union, the supervisory authorities shall cooperate with each other and, where relevant, with the Commission, through the consistency mechanism as set out in this Section.

유럽연합 전역에 본 규정을 일관되게 적용하기 위해, 감독기관들은 본 절에 명시된 일관성 메커니즘을 통해 상호 간에, 그리고 적정한 경우 집행위원회와 협력해야 한다.

Article 64
Opinion of the Board

제64조
유럽정보보호이사회 의견

1. The Board shall issue an opinion where a competent supervisory authority intends to adopt any of the measures below. To that end, the competent supervisory authority shall communicate the draft decision to the Board, when it:

   (a) aims to adopt a list of the processing operations subject to the requirement for a data protection impact assessment pursuant to Article 35(4);

   (b) concerns a matter pursuant to Article 40(7) whether a draft code of conduct or an amendment or extension to a code of conduct complies with this Regulation;

   (c) aims to approve the criteria for accreditation of a body pursuant to Article 41(3) or a certification body pursuant to Article 43(3);

   (d) aims to determine standard data protection clauses referred to in point (d) of Article 46(2) and Article 28(8);

   (e) aims to authorise contractual clauses referred to in point (a) of Article 46(3); or

   (f) aims to approve binding corporate rules within the meaning of Article 47.

1. 유럽정보보호이사회는 관할 감독기관이 다음의 조치 중 어느 한 가지를 채택하고자 할 경우 의견서를 발부해야 한다. 이를 위해 관할 감독기관은 다음의 경우 결정(안)을 유럽 정보보호이사회에 제출해야 한다.

   (a) 제35조(4)에 의거한 개인정보 보호 영향평가 요건을 따르는 정보처리 작업 목록을 채택하고자 할 경우

   (b) 행동강령(안) 또는 행동강령 개정판이나 확장판이 본 규정을 준수하는지 여부의, 제40(7)조에 따른 사안에 관한 경우

   (c) 제41조(3)에 의거한 기구 또는 제43조(3)에 의거한 인증 기구의 인증 기준을 승인하고자 할 경우

   (d) 제46조(2) (d)호와 제28조(8)에 명시된 정보보호 표준조항을 결정하고자 할 경우

   (e) 제46조(3) (a)호에 명시된 계약 조항을 승인하고자 할 경우

   (f) 제47조에 규정된 의무적 기업 규칙을 승인하고자 할 경우

2. Any supervisory authority, the Chair of the Board or the Commission may request that any matter of general application or producing effects in more than one Member State be examined by the Board with a view to obtaining an opinion, in particular where a competent supervisory authority does not comply with the obligations for mutual assistance in accordance with Article 61 or for joint operations in accordance with Article 62.

2. 특히 관할 감독기관이 제61조에 따른 상호 지원의 의무나 제62조에 따른 공동 작업의 의무를 준수하지 않는 경우, 감독기관, 유럽정보보호이사회 의장 또는 집행위원회는 의견수렴을 위해 하나 이상의 회원국에서의 일반적 적용 또는 효력 발생의 사안을 유럽정보보호이사회가 검토해 줄 것을 요청할 수 있다.

3. In the cases referred to in paragraphs 1 and 2, the Board shall

3. 제1항 및 제2항에 명시된 사례의 경우, 유럽정보보호이사회는 동일 사

issue an opinion on the matter submitted to it provided that it has not already issued an opinion on the same matter. That opinion shall be adopted within eight weeks by simple majority of the members of the Board. That period may be extended by a further six weeks, taking into account the complexity of the subject matter. Regarding the draft decision referred to in paragraph 1 circulated to the members of the Board in accordance with paragraph 5, a member which has not objected within a reasonable period indicated by the Chair, shall be deemed to be in agreement with the draft decision.	안에 대해 이미 의견서를 발부하지 않았다면 제출 받은 사안에 대해 의견서를 발부해야 한다. 그 의견서는 8주 내에 유럽정보보호이사회의 단순 과반수로 채택되어야 한다. 본 기간은 사안의 복잡성을 참작하여 6주간 추가 연장될 수 있다. 제1항에 명시되고 제5항에 따라 이사회 소속 위원에게 회람되는 결정(안)에 대해 의장이 적시한 적정 기간 내에 반대하지 않는 위원은 결정(안)에 동의한 것으로 간주한다.
4. Supervisory authorities and the Commission shall, without undue delay, communicate by electronic means to the Board, using a standardised format any relevant information, including as the case may be a summary of the facts, the draft decision, the grounds which make the enactment of such measure necessary, and the views of other supervisory authorities concerned.	4. 감독기관과 집행위원회는 경우에 따라 사실 요약, 결정(안), 그 같은 조치의 제정을 필요로 하게 된 근거, 그리고 기타 관련 감독기관들의 견해를 포함한 관련 정보를 전자적 수단으로 표준화된 형식을 사용하여 유럽정보보호이사회에 부당한 지체 없이 전달해야 한다.
5. The Chair of the Board shall, without undue, delay inform by electronic means: (a) the members of the Board and the Commission of any relevant information which has been communicated to it using a standardised format. The secretariat of the Board shall, where necessary, provide translations of relevant information; and (b) the supervisory authority referred to, as the case may be, in paragraphs 1 and 2, and the Commission of the opinion and make it public.	5. 유럽정보보호이사회 의장은 부당한 지체 없이 다음의 내용을 통지해야 한다. (a) 유럽정보보호이사회 위원 및 집행위원회에 표준화된 양식을 사용하여 전달된 관련 정보 일체. 유럽정보보호이사회 사무국은 필요한 경우 관련 정보의 번역본을 제공해야 한다. (b) 제1항 및 제2항에 명시된 해당 감독기관과 집행위원회에 의견서 통지 및 일반 공개
6. The competent supervisory authority shall not adopt its draft decision referred to in paragraph 1 within the period referred to in paragraph 3.	6. 제3항에 명시된 기간 내에 관할 감독기관은 제1항에 명시된 결정(안)을 채택해서는 아니 된다.
7. The supervisory authority referred to in paragraph 1 shall take utmost account of the opinion of the Board and shall within two weeks after receiving the opinion, electronically communicate to the Chair of the Board whether it maintains or will amend its draft decision and, if any, the amended draft decision, using a standardised format.	7. 제1항에 명시된 감독기관은 의견서 접수 후 2주 내에 유럽정보보호이사회의 의견을 신중하게 고려한 후 유럽정보보호이사회 의장에게 결정(안)을 유지할 것인지 또는 수정할 것인지 여부를 전자적 수단으로 통보하고, 수정할 경우 표준화된 양식을 활용하여 수정한 결정(안)을 전달해야 한다.
8. Where the supervisory authority concerned informs the Chair of the Board within the period referred to in paragraph 7 of this Article that it does not intend to follow the opinion of the Board, in whole or in part, providing the relevant grounds, Article 65(1) shall apply.	8. 관련 감독기관이 제7항에 명시된 기간 내에 유럽정보보호이사회 의장에게 이사회 의견의 전부 또는 일부를 따르지 않겠다는 의사를 적정한 근거와 함께 통보하는 경우, 제65조(1)이 적용되어야 한다.

Article 65 Dispute resolution by the Board	제65조 유럽정보보호이사회의 분쟁 해결
1. In order to ensure the correct and consistent application of this Regulation in individual cases, the Board shall adopt a binding decision in the following cases: (a) where, in a case referred to in Article 60(4), a supervisory authority concerned has raised a relevant and reasoned objection to a draft decision of the lead authority or the lead authority has rejected an objection as being not relevant or reasoned. The binding decision shall concern all the matters which are the subject of the relevant and reasoned objection, in particular whether there is an infringement of this Regulation; (b) where there are conflicting views on which of the supervisory authorities concerned is competent for the main establishment; (c) where a competent supervisory authority does not request the opinion of the Board in the cases referred to in Article 64(1), or does not follow the opinion of the Board issued under Article 64. In that case, any supervisory authority concerned or the Commission may communicate the matter to the Board.	1. 개별 사례에서 본 규정을 정확하고 일관되게 적용하기 위해, 유럽정보보호이사회는 다음과 같은 경우 구속력 있는 결정을 채택해야 한다. (a) 제60조(4)의 사례의 경우 관련 감독기관이 선임 감독기관의 결정(안)에 적정하고 타당한 이의를 표명하거나 선임 감독기관이 해당 이의가 적정 또는 타당하지 않다고 거부하는 경우. 구속력 있는 결정은 본 규정의 침해 여부 등 적정하고 타당한 이의의 대상이 되는 모든 사안에 관한 것이어야 한다. (b) 주 사업장을 관할하는 관련 감독기관들의 의견이 충돌하는 경우 (c) 제64조(1)의 사례에서 관할 감독기관이 유럽정보보호이사회에 의견을 요청하지 않거나 제64조로 발부된 유럽정보보호이사회의 의견에 따르지 않을 경우. 이 같은 경우, 관련 감독기관이나 집행위원회는 유럽정보보호이사회에 해당 사안을 전달할 수 있다.
2. The decision referred to in paragraph 1 shall be adopted within one month from the referral of the subject-matter by a two-third majority of the members of the Board. This period may be extended by a further month on account of the complexity of the subject-matter. The decision referred to in paragraph 1 shall be reasoned and addressed to the lead supervisory authority and all the supervisory authorities concerned and binding on them.	2. 제1항에 명시된 결정은 유럽정보보호이사회 위원의 2/3 다수결에 의해 사안의 상정 후 1개월 이내에 채택되어야 한다. 이 기간은 사안의 복잡성을 감안하여 1개월간 추가 연장될 수 있다. 제1항에 명시된 결정은 타당하고 선임 감독기관과 모든 관련 감독기관을 대상으로 해야 하며 이들에게 구속력을 가져야 한다.
3. Where the Board has been unable to adopt a decision within the periods referred to in paragraph 2, it shall adopt its decision within two weeks following the expiration of the second month referred to in paragraph 2 by a simple majority of the members of the Board. Where the members of the Board are split, the decision shall by adopted by the vote of its Chair.	3. 유럽정보보호이사회는 제2항에 명시된 기간 내에 결정문을 채택할 수 없을 경우, 제2항에 명시된 두 번째 달의 만료 후 2주 이내에 위원회 단순 다수결로 결정문을 채택해야 한다. 이사회 위원들이 분열될 경우, 의장의 의결로 결정문을 채택해야 한다.
4. The supervisory authorities concerned shall not adopt a decision on the subject matter submitted to the Board under paragraph 1 during the periods referred to in paragraphs 2 and 3.	4. 관련 감독기관은 제2항 및 제3항에 명시된 기간 동안 제1항에 따라 유럽정보보호이사회에 제출된 사안에 대하여 결정을 채택해서는 안 된다.
5. The Chair of the Board shall notify, without undue delay, the decision referred to in paragraph 1 to the supervisory authorities concerned. It shall inform the Commission thereof. The decision shall be published on the website of the Board without delay after the supervisory authority has notified the final decision referred to in paragraph 6.	5. 유럽정보보호이사회 의장은 제1항에 명시된 결정을 부당한 지체 없이 관련 감독기관에게 통보해야 한다. 집행위원회에도 통보해야 한다. 감독기관이 제6항에 명시된 최종 결정을 통보한 후 이는 지체 없이 유럽정보보호이사회 웹사이트에 게재되어야 한다.

6. The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged shall adopt its final decision on the basis of the decision referred to in paragraph 1 of this Article, without undue delay and at the latest by one month after the Board has notified its decision. The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged, shall inform the Board of the date when its final decision is notified respectively to the controller or the processor and to the data subject. The final decision of the supervisory authorities concerned shall be adopted under the terms of Article 60(7), (8) and (9). The final decision shall refer to the decision referred to in paragraph 1 of this Article and shall specify that the decision referred to in that paragraph will be published on the website of the Board in accordance with paragraph 5 of this Article. The final decision shall attach the decision referred to in paragraph 1 of this Article.	6. 선임 감독기관 또는 경우에 따라 민원을 접수한 감독기관은 제1항에 명시된 결정을 근거로 부당한 지체 없이, 늦어도 유럽정보보호이사회가 결정을 게재한 후 1개월 이내에 최종 결정을 채택해야 한다. 선임 감독기관 또는 경우에 따라 민원을 접수한 감독기관은 최종 결정이 개인정보처리자나 수탁처리자 및 개인정보주체에 각각 고지되는 날짜를 유럽정보보호이사회에 통보해야 한다. 관련 감독기관들의 최종 결정은 제60조(7), (8) 및 (9)항의 조건으로 채택되어야 한다. 최종 결정은 제1항에 명시된 결정을 지칭하며, 제5항에 따라 유럽정보보호이사회 웹사이트에 제1항의 결정이 게재될 것임을 명시해야 한다. 최종 결정에는 제1항에 명시된 결정이 첨부되어야 한다.
Article 66 **Urgency procedure**	**제66조** **긴급성(시급성) 절차**
1. In exceptional circumstances, where a supervisory authority concerned considers that there is an urgent need to act in order to protect the rights and freedoms of data subjects, it may, by way of derogation from the consistency mechanism referred to in Articles 63, 64 and 65 or the procedure referred to in Article 60, immediately adopt provisional measures intended to produce legal effects on its own territory with a specified period of validity which shall not exceed three months. The supervisory authority shall, without delay, communicate those measures and the reasons for adopting them to the other supervisory authorities concerned, to the Board and to the Commission.	1. 예외적인 상황에서 관련 감독기관이 개인정보주체의 권리와 자유를 보호하기 위해 시급히 조치를 취해야 필요가 있다고 판단할 경우, 제63조, 제65조 및 제65조의 일관성 메커니즘이나 제60조에 명시된 절차의 적용을 일부 제외하여, 법적 효력을 발생시킬 의도의 잠정적 조치를 자국의 영토에서 3개월을 초과하지 않는 유효 기간을 지정하여 즉시 채택할 수 있다. 감독기관은 지체 없이 해당 조치 및 조치의 채택 사유를 나머지 감독기관, 유럽정보보호이사회 및 집행위원회에 전달해야 한다.
2. Where a supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion or an urgent binding decision from the Board, giving reasons for requesting such opinion or decision.	2. 감독기관이 제1항에 따른 조치를 취하고 최종 조치를 시급히 채택해야 한다고 판단할 경우, 유럽정보보호이사회에 긴급한 의견 또는 법적 구속력이 있는 결정을 요청할 수 있고 이 때 그 같은 의견이나 결정의 요청 사유를 제공해야 한다.
3. Any supervisory authority may request an urgent opinion or an urgent binding decision, as the case may be, from the Board where a competent supervisory authority has not taken an appropriate measure in a situation where there is an urgent need to act, in order to protect the rights and freedoms of data subjects, giving reasons for requesting such opinion or decision, including for the urgent need to act.	3. 관할 감독기관이 개인정보주체의 권리와 자유를 보호하기 위해 시급히 조치를 취해야 하는 상황에서 적절한 조치를 취하지 못한 경우, 어느 감독기관이라도 경우에 따라 유럽정보보호이사회에 긴급한 의견 또는 법적 구속력이 있는 결정을 요청할 수 있고 이 때 시급한 조치의 필요성 등 그 같은 의견이나 결정의 요청 사유를 제공해야 한다.
4. By derogation from Articles 64(3) and 65(2), an urgent opinion or an urgent binding decision referred to in paragraphs 2 and 3 of this Article shall be adopted within two weeks by simple majority of the members of the Board.	4. 제64조(3) 및 제65조(2)의 적용을 일부 제외하여, 본 조 제2항 및 제3항에 명시된 긴급한 의견이나 법적 구속력이 있는 결정은 2주 이내에 이사회 위원들의 단순 다수결로 채택되어야 한다.

Article 67 **Exchange of information**	**제67조** **정보의 교환**
The Commission may adopt implementing acts of general scope in order to specify the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board, in particular the standardised format referred to in Article 64. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).	집행위원회는 감독기관들 간, 그리고 감독기관과 유럽정보보호이사회 간에 제64조에 명시된 표준화된 양식 등 전자적 수단으로 정보를 교환하기 위한 방식을 규정하기 위해 일반적 범위의 이행 법률을 채택할 수 있다. 그 같은 이행 법률은 제93조(2)에 명시된 검토절차에 따라 채택되어야 한다.
SECTION 3 **EUROPEAN DATA PROTECTION BOARD**	**제3절** **유럽정보보호이사회**
Article 68 **European Data Protection Board**	**제68조** **유럽정보보호이사회**
1. The European Data Protection Board (the 'Board') is hereby established as a body of the Union and shall have legal personality.	1. 유럽정보보호이사회(이사회)를 유럽연합 기구로 정하고 법인격을 가지도록 한다.
2. The Board shall be represented by its Chair.	2. 이사회는 의장이 대표한다.
3. The Board shall be composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor, or their respective representatives.	3. 이사회는 각 회원국 감독기관의 장과 유럽정보보호감독기구(European Data Protection Supervisor), 또는 각 대리인으로 구성된다.
4. Where in a Member State more than one supervisory authority is responsible for monitoring the application of the provisions pursuant to this Regulation, a joint representative shall be appointed in accordance with that Member State's law.	4. 한 회원국에서 하나 이상의 감독기관이 본 규정에 따른 조문의 적용을 모니터링 할 책임이 있는 경우, 해당 회원국의 법률에 따라 공동 대리인이 임명되어야 한다.
5. The Commission shall have the right to participate in the activities and meetings of the Board without voting right. The Commission shall designate a representative. The Chair of the Board shall communicate to the Commission the activities of the Board.	5. 집행위원회는 의결권 없이 이사회의 활동 및 회의에 참석할 권리가 있다. 집행위원회는 대리인을 지정해야 한다. 이사회 의장은 집행위원회에 이사회 활동을 통보해야 한다.
6. In the cases referred to in Article 65, the European Data Protection Supervisor shall have voting rights only on decisions which concern principles and rules applicable to the Union institutions, bodies, offices and agencies which correspond in substance to those of this Regulation.	6. 제65조에 명시된 사례의 경우, 유럽정보보호감독기구는 유럽연합 산하기관, 기구, 사무소 및 에이전시에 적용되고 사실상 본 규정에 상응하는 원칙 및 규정에 관한 결정에 대해서만 의결권을 갖는다.

Article 69 Independence	제69조 독립성
1. The Board shall act independently when performing its tasks or exercising its powers pursuant to Articles 70 and 71.	1. 유럽정보보호이사회는 제70조 및 제71조에 따른 임무를 수행하거나 권한을 행사할 때 독립적으로 활동한다.
2. Without prejudice to requests by the Commission referred to in point (b) of Article 70(1) and in Article 70(2), the Board shall, in the performance of its tasks or the exercise of its powers, neither seek nor take instructions from anybody.	2. 제70조(1) (b)호 및 제70조(2)에 명시된 집행위원회의 요청을 침해하지 아니하여, 유럽정보보호이사회는 임무를 수행하거나 권한을 행사하는 중에 다른 어느 누구로부터도 지시를 구하거나 그들의 지시를 따르지 아니한다.
Article 70 Tasks of the Board	**제70조 유럽정보보호이사회의 업무**
1. The Board shall ensure the consistent application of this Regulation. To that end, the Board shall, on its own initiative or, where relevant, at the request of the Commission, in particular: (a) monitor and ensure the correct application of this Regulation in the cases provided for in Articles 64 and 65 without prejudice to the tasks of national supervisory authorities; (b) advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Regulation; (c) advise the Commission on the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules; (d) issue guidelines, recommendations, and best practices on procedures for erasing links, copies or replications of personal data from publicly available communication services as referred to in Article 17 (2); (e) examine, on its own initiative, on request of one of its members or on request of the Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best practices in order to encourage consistent application of this Regulation; (f) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for further specifying the criteria and conditions for decisions based on profiling pursuant to Article 22(2); (g) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for establishing the personal data breaches and determining the undue delay referred to in Article 33(1) and (2) and for the particular circumstances in which a controller or a processor is required to notify the personal data breach; (h) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph as to the	1. 유럽정보보호이사회는 본 규정이 일관적으로 적용되도록 해야 한다. 이를 위해 이사회는 자발적으로 또는 적정한 경우 집행위원회의 요청에 따라, 특히 다음의 업무를 수행한다. (a) 국가 감독기관의 업무를 침해하지 아니하고 제64조 및 제65조에 규정된 경우에서 본 규정의 올바른 적용 여부를 모니터링하고 보장한다. (b) 본 규정의 개정안을 포함하여 유럽연합 역내의 개인정보 보호와 관련된 문제에 대해 집행위원회에 자문을 제공한다. (c) 의무적 기업 규칙에 관해 개인정보처리자, 수탁처리자, 감독기관 간에 이루어지는 정보 교환의 양식 및 절차에 대해 집행위원회에 자문을 제공한다. (d) 제17조(2)에 명시된 대로 일반에 공개되는 통신 서비스로부터 개인정보의 링크, 사본 또는 복제본을 삭제하기 위한 절차에 대해 가이드라인, 권고사항 및 모범사례를 발행한다. (e) 자발적으로 또는 소속 위원의 요청에 따라 또는 집행위원회의 요청에 따라 본 규정의 적용에 대한 질의사항을 검토하고 본 규정의 일관적 적용을 장려하기 위해 가이드라인, 권고사항 및 모범사례를 발행한다. (f) 제22조(2)에 따른 프로파일링을 기반으로 하는 결정의 기준 및 조건을 추가로 명시하기 위해 본 항 (e)호에 부합하는 가이드라인, 권고사항 및 모범사례를 발행한다. (g) 개인정보 침해를 규명하고 제33조(1) 및 (2)항에 명시된 부당한 지체를 결정하기 위해서, 그리고 개인정보처리자 또는 수탁처리자가 개인정보 침해에 대해 고지해야 하는 특정 상황에 대하여 본 항 (e)호에 부합하는 가이드라인, 권고사항 및 모범사례를 발행한다. (h) 개인정보 침해가 제34조(1)에 명시된 개인의 권리와 자유에 대한 중대한 위험을 초래할 가능성이 있는 상황에 대해 본 항 (e)호에 부합하는 가이드라인, 권고사항 및 모범사례를 발행한다. (i) 개인정보처리자가 준수하는 의무적 기업 규칙과 수탁처리자가 준수하는 의무적 기업 규칙 및 제47조에 명시된 관련 개인정보주체의 개인정보 보호를 보장하기 위한 추가적 필요요건을 기반으로 개인정보 이전의 기준 및 요건을 추가로 명시하기 위해 본 항 (e)호에 부합하는 가이드라인, 권고사항 및 모범사례를 발행한다.

circumstances in which a personal data breach is likely to result in a high risk to the rights and freedoms of the natural persons referred to in Article 34(1).

(i) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for the purpose of further specifying the criteria and requirements for personal data transfers based on binding corporate rules adhered to by controllers and binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned referred to in Article 47;

(j) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for the purpose of further specifying the criteria and requirements for the personal data transfers on the basis of Article 49(1);

(k) draw up guidelines for supervisory authorities concerning the application of measures referred to in Article 58(1), (2) and (3) and the fixing of administrative fines pursuant to Articles 83;

(l) review the practical application of the guidelines, recommendations and best practices referred to in point (e) and (f);

(m) issue guidelines, recommendations and best practices in accordance with point (e) of this paragraph for establishing common procedures for reporting by natural persons of infringements of this Regulation pursuant to Article 54(2);

(n) encourage the drawing-up of codes of conduct and the establishment of data protection certification mechanisms and data protection seals and marks pursuant to Articles 40 and 42;

(o) carry out the accreditation of certification bodies and its periodic review pursuant to Article 43 and maintain a public register of accredited bodies pursuant to Article 43(6) and of the accredited controllers or processors established in third countries pursuant to Article 42(7);

(p) specify the requirements referred to in Article 43(3) with a view to the accreditation of certification bodies under Article 42;

(q) provide the Commission with an opinion on the certification requirements referred to in Article 43(8);

(r) provide the Commission with an opinion on the the icons referred to in Article 12(7);

(s) provide the Commission with an opinion for the assessment of the adequacy of the level of protection in a third country or international organisation, including for the assessment whether a third country, a territory or one or more specified sectors within that third country, or an international organisation no longer ensures an adequate level of protection. To that end, the Commission shall provide the Board with all necessary documentation, including correspondence with the government of the third country, with regard to that third country, territory or specified sector, or with the international organisation.

(j) 제49조(1)를 근거로 하는 개인정보 이전에 대한 기준 및 요건을 추가로 명시하기 위해 본 항 (e)호에 부합하는 가이드라인, 권고사항 및 모범사례를 발행한다.

(k) 감독기관을 위해 제58조(1), (2) 및 (3)항에 명시된 조치의 적용 및 제83조에 따른 행정 과태료 책정에 관한 가이드라인을 수립한다.

(l) (e)호 및 (f)호에 명시된 가이드라인, 권고사항 및 모범사례의 실제 적용을 검토한다.

(m) 제54조(2)에 따라 개인이 본 규정의 침해를 신고하기 위한 보편적 절차 수립에 대해 본 항 (e)호에 부합하는 가이드라인, 권고사항 및 모범사례를 발행한다.

(n) 제40조 및 제42조에 따른 행동강령의 수립 및 개인정보보호 인증 메커니즘, 보호 인장과 마크의 구축을 장려한다.

(o) 제43조에 따라 인증기관의 승인 및 정기 검토를 실시하고 제43조(6)에 따라 인증된 기관 및 제42조(7)에 따라 제3국에 설립된 공인 개인정보처리자 또는 수탁처리자의 공공기록부(public register)를 유지한다.

(p) 제42조에 따라 인증기관의 승인을 목적으로 제43조(3)에 명시된 요건을 지정한다.

(q) 제43조(8)에 명시된 인증 요건에 관한 의견서를 집행위원회에 제공한다.

(r) 제12조(7)에 명시된 아이콘에 관한 의견서를 집행위원회에 제공한다.

(s) 제3국, 해당 제3국의 영토나 하나 이상의 지정 부문, 또는 국제기구가 더 이상 적정한 보호 수준을 보장하지 않는지에 대한 평가를 비롯하여 제3국이나 국제기구에서 시행되는 보호 수준의 적정성 평가에 대한 의견서를 집행위원회에 제공한다. 이를 위해 집행위원회는 제3국 정부나 해당 제3국의 영토나 지정 부문, 또는 국제기구와 주고받은 서한 등 필요한 문서 일체를 유럽정보보호이사회에 제공해야 한다.

(t) 제64조(2)에 의거하여 제출된 사안에 대하여, 그리고 제66조에 명시된 사례들의 경우에서 제65조에 따라 구속력 있는 결정을 발부하기 위해 제64조(1)에 명시된 일관성 메커니즘에 따라 감독기관의 결정(안)에 관한 의견서를 발행한다.

(u) 감독기관들 사이에서의 협력 및 효과적인 양자간 및 다자간 정보와 모범사례 교류를 촉진시킨다.

(v) 공통의 교육 프로그램을 장려하고 감독기관들 간에, 그리고 적절한 경우 제3국의 감독기관들이나 국제기구와의 인적 교류를 용이하게 한다.

(w) 전 세계 개인정보보호 감독기관들과의 정보보호 법률 및 관행에 대한 지식과 자료의 교류를 촉진시킨다.

(x) 제40조(9)에 따라 유럽연합 차원에서 수립된 행동강령에 관한 의견서를 발부한다.

(y) 일관성 메커니즘에서 처리되는 사안에 대하여 감독기관 및 법원이 채택한 결정의 공개 전자 기록부(electronic register)를 유지한다.

(t) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 64(1), on matters submitted pursuant to Article 64(2) and to issue binding decisions pursuant to Article 65, including in cases referred to in Article 66; (u) promote the cooperation and the effective bilateral and multilateral exchange of information and best practices between the supervisory authorities; (v) promote common training programmes and facilitate personnel exchanges between the supervisory authorities and, where appropriate, with the supervisory authorities of third countries or with international organisations; (w) promote the exchange of knowledge and documentation on data protection legislation and practice with data protection supervisory authorities worldwide. (x) issue opinions on codes of conduct drawn up at Union level pursuant to Article 40(9); and (y) maintain a publicly accessible electronic register of decisions taken by supervisory authorities and courts on issues handled in the consistency mechanism.	
2. Where the Commission requests advice from the Board, it may indicate a time limit, taking into account the urgency of the matter.	2. 집행위원회가 유럽정보보호이사회의 자문을 요청하는 경우, 사안의 시급성을 감안하여 시한을 명시할 수 있다.
3. The Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee referred to in Article 93 and make them public.	3. 유럽정보보호이사회는 집행위원회와 제93조에 명시된 위원회(committee)에 이사회의 의견, 가이드라인, 권고사항 및 모범사례를 전달해야 한다.
4. The Board shall, where appropriate, consult interested parties and give them the opportunity to comment within a reasonable period. The Board shall, without prejudice to Article 76, make the results of the consultation procedure publicly available.	4. 유럽정보보호이사회는 적절한 경우 이해당사자와 협의하고 적정한 기간 내에 의견을 개진할 기회를 제공해야 한다. 이사회는 제76조를 침해하지 않고 협의 절차의 결과를 공개해야 한다.
Article 71 **Reports**	**제71조** **보고서**
1. The Board shall draw up an annual report regarding the protection of natural persons with regard to processing in the Union and, where relevant, in third countries and international organisations. The report shall be made public and be transmitted to the European Parliament, to the Council and to the Commission.	1. 유럽정보보호이사회는 유럽연합 및 적절한 경우 제3국과 국제기구에서의 개인정보 처리와 관련해 개인의 보호에 관한 연례 보고서를 작성해야 한다. 보고서는 일반에 공개되고 유럽의회, 각료이사회 및 집행위원회에 전달해야 한다.
2. The annual report shall include a review of the practical application of the guidelines, recommendations and best practices referred to in point (l) of Article 70(1) as well as of the binding decisions referred to in Article 65.	2. 연례 보고서에는 제70(1)조의 (l)호에 명시된 가이드라인, 권고사항과 모범사례 및 제65조에 명시된 법적 구속력이 있는 결정의 실제 적용에 관한 검토가 포함되어야 한다.

Article 72 **Procedure**	**제72조** **절차**
1. The Board shall take decisions by a simple majority of its members, unless otherwise provided for in this Regulation.	1. 유럽정보보호이사회는 본 규정에서 별도로 규정하지 않는 한 이사회 위원의 단순 다수결로 결정을 내린다.
2. The Board shall adopt its own rules of procedure by a two-third majority of its members and organise its own operational arrangements.	2. 유럽정보보호이사회는 위원의 2/3 다수결로 자체적인 절차 규정을 채택하고 자체적인 운영 방식을 조직한다.
Article 73 **Chair**	**제73조** **의장**
1. The Board shall elect a chair and two deputy chairs from amongst its members by simple majority.	1. 유럽정보보호이사회는 위원들 중에서 단순 다수결로 의장 1인과 부의장 2인을 선출한다.
2. The term of office of the Chair and of the deputy chairs shall be five years and be renewable once.	2. 의장과 부의장의 임기는 5년으로 하고 1회 연임이 가능하다.
Article 74 **Tasks of the Chair**	**제74조** **의장의 역할**
1. The Chair shall have the following tasks: (a) to convene the meetings of the Board and prepare its agenda; (b) to notify decisions adopted by the Board pursuant to Article 65 to the lead supervisory authority and the supervisory authorities concerned; (c) to ensure the timely performance of the tasks of the Board, in particular in relation to the consistency mechanism referred to in Article 63.	1. 의장은 다음의 업무를 수행해야 한다. (a) 유럽정보보호이사회 회의를 소집하고 안건을 준비한다. (b) 제65조에 의거하여 유럽정보보호이사회가 채택한 결정을 선임 감독기관 및 관련 감독기관에 통보한다. (C) 특히 제63조의 일관성 메커니즘과 관련해 유럽정보보호이사회의 업무가 적시에 수행되도록 한다.
2. The Board shall lay down the allocation of tasks between the Chair and the deputy chairs in its rules of procedure.	2. 유럽정보보호이사회는 이사회의 절차 규정에 의장과 부의장 간의 업무 분장을 규정해야 한다.
Article 75 **Secretariat**	**제75조** **사무국**
1. The Board shall have a secretariat, which shall be provided by the European Data Protection Supervisor.	1. 유럽정보보호이사회는 유럽정보보호감독기구가 제공하는 사무국을 둔다.

2. The secretariat shall perform its tasks exclusively under the instructions of the Chair of the Board.	2. 사무국은 이사회 의장의 지시에 따라 독자적으로 업무를 수행한다.
3. The staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation shall be subject to separate reporting lines from the staff involved in carrying out tasks conferred on the European Data Protection Supervisor.	3. 본 규정이 유럽정보보호이사회에 부여한 업무를 수행하는데 관여하는 유럽정보보호감독기구의 직원은 유럽정보보호감독기구에 부여된 업무의 수행에 관여하는 직원과 별도의 보고 체계를 따라야 한다.
4. Where appropriate, the Board and the European Data Protection Supervisor shall establish and publish a Memorandum of Understanding implementing this Article, determining the terms of their cooperation, and applicable to the staff of the European Data Protection Supervisor involved in carrying out the tasks conferred on the Board by this Regulation.	4. 적절한 경우, 유럽정보보호이사회와 유럽정보보호감독기구는 본 조문을 이행하는 양해각서를 체결 및 발표해야 한다. 양해각서는 협력 조건을 결정하고 본 규정이 유럽정보보호이사회에 부여한 업무를 수행하는데 관여하는 유럽정보보호감독기구 직원에 적용된다.
5. The secretariat shall provide analytical, administrative and logistical support to the Board.	5. 사무국은 유럽정보보호이사회에 분석적, 행정적, 로지스틱 관련 지원을 제공해야 한다.
6. The secretariat shall be responsible in particular for: (a) the day-to-day business of the Board; (b) communication between the members of the Board, its Chair and the Commission; (c) communication with other institutions and the public; (d) the use of electronic means for the internal and external communication; (e) the translation of relevant information; (f) the preparation and follow-up of the meetings of the Board; (g) the preparation, drafting and publication of opinions, decisions on the settlement of disputes between supervisory authorities and other texts adopted by the Board.	6. 사무국은 특히 다음에 대한 책임이 있다. (a) 유럽정보보호이사회의 일일 업무 (b) 유럽정보보호이사회 위원들, 의장 및 유럽집행위원회 간의 소통 (c) 기타 기구 및 일반과의 소통 (d) 내·외부 소통을 위한 전자적 수단 활용 (e) 관련 정보의 번역 (f) 유럽정보보호이사회 회의 준비 및 후속 조치 (g) 의견서, 감독기관들 간의 분쟁 해결에 대한 결정, 및 이사회가 채택한 기타 문서의 준비, 초안 마련 및 발표
Article 76 **Confidentiality**	**제76조** **기밀성**
1. The discussions of the Board shall be confidential where the Board deems it necessary, as provided for in its rules of procedure.	1. 유럽정보보호이사회는 절차 규정에 규정된 바와 같이 필요하다고 판단하는 경우 이사회의 논의를 기밀로 해야 한다.
2. Access to documents submitted to members of the Board, experts and representatives of third parties shall be governed by Regulation (EC) No 1049/2001 of the European Parliament and of the Council1.	2. 유럽정보보호이사회 위원, 전문가 및 제3자의 대리인에게 제출된 문서의 열람은 유럽의회 및 각료이사회 규정서 (EC) No 1049/2001의 규제를 받는다.

CHAPTER VIII REMEDIES, LIABILITY AND PENALTIES	제VIII장 구제책, 책임, 처벌
Article 77 Right to lodge a complaint with a supervisory authority	제77조 감독기관에 민원을 제기할 권리
1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringment if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.	1. 다른 행정적 또는 법적 구제책을 침해하지 아니하여, 모든 개인정보주체는 본인에 관한 개인정보의 처리가 본 규정을 침해한다고 판단될 경우 특히 거주지, 근무지 또는 침해 발생 의혹이 있는 장소가 소재한 회원국의 감독기관에 민원을 제기할 권리가 있다.
2. The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78.	2. 민원을 접수한 감독기관은 제78조에 의거한 법적 구제책의 가능성 등 민원 처리 경과 및 결과를 민원인에게 통보해야 한다.
Article 78 Right to an effective judicial remedy against a supervisory authority	제78조 감독기관에 대한 효과적인 사법구제권
1. Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.	1. 기타 행정적 또는 법적 구제책을 침해하지 아니하여, 각 개인이나 법인은 본인에 관한 감독기관의 법적 구속력 있는 결정에 반대하는 효과적인 법적 구제책을 가질 권리가 있다.
2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to a an effective judicial remedy where the supervisory authority which is competent pursuant to Article 55 and Article 56 does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged pursuant to Article 77.	2. 기타 행정적 또는 법적 구제책을 침해하지 아니하여, 각 개인정보주체는 제55조 및 제56조에 따른 관할 감독기관이 민원을 처리하지 않거나 3개월 이내에 개인정보주체에 제77조에 따라 접수된 민원의 처리 경과 또는 결과를 통보하지 않을 경우, 법적 구제책을 가질 권리가 있다.
3. Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.	3. 감독기관을 상대로 하는 법적 절차는 해당 감독기관이 설립된 회원국의 법정에서 진행된다.
4. Where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or a decision of the Board in the consistency mechanism, the supervisory authority shall forward that opinion or decision to the court.	4. 일관성 메커니즘에서 유럽정보보호이사회의 의견이나 결정에 이은 감독기관의 결정에 대하여 법적 절차가 제기될 경우, 감독기관은 그 의견이나 결정을 법원에 전달해야 한다.

Article 79 **Right to an effective judicial remedy against a controller or processor**	**제79조** **개인정보처리자나 수탁처리자를 상대로 한 효과적인 사법구제권**
1. Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.	1. 제77조에 따른 감독기관에 민원을 제기할 권리 등 가용할 수 있는 행정적 또는 법률외적 구제책을 침해하지 아니하여, 각 개인정보주체는 본인에 관한 개인정보의 처리가 본 규정을 준수하지 않음으로 인해 본 규정에 의거한 본인의 권리가 침해되었다고 판단될 경우 사법적 구제책을 가질 권리가 있다.
2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.	2. 개인정보처리자 또는 수탁처리자를 상대로 한 법적 절차는 해당 개인정보처리자 또는 수탁처리자의 사업장이 있는 회원국의 법정에서 진행되어야 한다. 그렇지 않으면 개인정보처리자나 수탁처리자가 공적 권한을 행사하는 회원국의 공공기관이 아닌 한 개인정보주체의 거주지가 있는 회원국의 법정에서 절차가 진행될 수도 있다.
Article 80 **Representation of data subjects**	**제80조** **개인정보주체의 대리**
1. The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.	1. 개인정보주체는 회원국 법률에 따라 적절히 구성되고 법정 목표가 공익에 있으며 개인정보 보호에 관한 개인정보주체의 권리 및 자유의 보호 분야에서 적극적으로 활동하는 비영리 기구, 조직 또는 협회에게 본인을 대신하여 민원을 제기하고 제77조, 제78조 및 제79조에 명시된 권리를 대신 행사하며 회원국 법률이 규정하는 경우 제82조에 명시된 보상 받을 권리를 대신 행사하도록 권한을 부여하는 권리를 가진다.
2. Member States may provide that any body, organisation or association referred to in paragraph 1 of this Article, independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority which is competent pursuant to Article 77 and to exercise the rights referred to in Articles 78 and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing.	2. 회원국은 개인정보 처리의 결과로 본 규정에 의거한 개인정보주체의 권리가 침해되었다고 판단될 경우, 본 조 제1항에 명시된 기구, 조직 또는 협회가 개인정보주체의 권한과 관계없이 자국에서 제77조에 따른 관할 감독기관에 민원을 제기할 권리를 가진다고 규정할 수 있다.

Article 81 Suspension of proceedings	제81조 법적 절차 중지
1. Where a competent court of a Member State has information on proceedings, concerning the same subject matter as regards processing by the same controller or processor, that are pending in a court in another Member State, it shall contact that court in the other Member State to confirm the existence of such proceedings.	1. 회원국의 관할 법원이 타 회원국의 법원에 계류 중인 동일한 개인정보처리자나 수탁처리자의 개인정보처리에 대하여 동일한 사안의 법적 절차에 관한 정보를 가지고 있는 경우, 그 회원국의 법원에 연락하여 해당 법적 절차의 존재 유무를 확인해야 한다.
2. Where proceedings concerning the same subject matter as regards processing of the same controller or processor are pending in a court in another Member State, any competent court other than the court first seized may suspend its proceedings.	2. 동일 개인정보처리자나 수탁처리자의 정보처리에 대하여 동일 사안에 관한 법적 절차가 타 회원국의 법원에 계류 중인 경우, 최초의 법원 외에 어느 관할 법원이라도 그 절차를 중지시킬 수 있다.
3. Where those proceedings are pending at first instance, any court other than the court first seized may also, on the application of one of the parties, decline jurisdiction if the court first seized has jurisdiction over the actions in question and its law permits the consolidation thereof.	3. 그 같은 절차가 제1심에서 계류 중인 경우, 최초 법원이 논의되는 조치에 대해 관할권을 가지고 있고 법률이 관할권의 통합을 허용한다면, 최초 법원 외에 어느 법원이라도 당사자 중 한 쪽의 신청으로 관할권을 거부할 수 있다.
Article 82 **Right to compensation and liability**	**제82조** **보상 권리 및 책임**
1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.	1. 본 규정의 침해로 인해 물질적 또는 비 물질적 피해를 입은 자는 누구든지 개인정보처리자 또는 수탁처리자로부터 피해 보상을 받을 권리가 있다.
2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.	2. 정보처리에 관여하는 개인정보처리자는 본 규정을 침해하는 정보처리로 초래된 피해에 대하여 책임을 져야 한다. 수탁처리자는 수탁처리자들에게 구체적으로 지시된 본 규정의 의무사항을 준수하지 않은 경우 또는 개인정보처리자의 합법적 지시를 벗어나거나 그 지시에 반대되는 행동을 한 경우에 한하여 정보처리로 초래된 피해에 대하여 책임을 져야 한다.
3. A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.	3. 피해를 초래한 사건에 대하여 어떠한 식으로도 책임이 없음을 증명할 경우, 개인정보처리자 또는 수탁처리자는 제2항에 의거한 책임에서 면제된다.
4. Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.	4. 하나 이상의 개인정보처리자 또는 수탁처리자가 동일한 정보처리에 관여하고 제2항 및 제3항에 따라 해당 정보처리로 초래된 피해에 대하여 책임이 있는 경우, 각 개인정보처리자나 수탁처리자는 개인정보주체의 유효한 보상을 보장하기 위해 피해 전체에 대하여 책임을 져야 한다.

5. Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2.	5. 개인정보처리자 또는 수탁처리자가 제4항에 따라 피해에 대해 전액 보상한 경우, 해당 개인정보처리자 또는 수탁처리자는 제2항에 명시된 조건에 부합하여 동일한 정보처리에 관여한 기타 개인정보처리자나 수탁처리자에게 피해에 대한 그들의 책임 상응하는 보상액 일부를 청구할 수 있다.
6. Court proceedings for exercising the right to receive compensation shall be brought before the courts competent under the law of the Member State referred to in Article 79(2).	6. 보상 받을 권리를 행사하기 위한 법정 절차는 제79조(2)에 명시된 회원국 법률에 따른 관할 법원에서 진행되어야 한다.
Article 83 **General conditions for imposing administrative fines**	**제83조** **행정 과태료 부과에 관한 일반 조건**
1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.	1. 각 감독기관은 제4항, 제5항 및 제6항에 명시된 본 규정의 침해와 관련하여, 본 조문에 따른 행정 과태료의 부과가 개별 사례에서 유효하고 비례적이며 (침해행위를 하지 않도록 하는) 설득력이 있도록 해야 한다.
2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following: (a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them; (b) the intentional or negligent character of the infringement; (c) any action taken by the controller or processor to mitigate the damage suffered by data subjects; (d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32; (e) any relevant previous infringements by the controller or processor; (f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement; (g) the categories of personal data affected by the infringement; (h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;	2. 행정 과태료는 각 개별 사례의 정황에 따라 제58조(2)의 (a)-(h)호 및 (j)호에 언급된 조치에 추가로 부과되거나 그 대신 부과되어야 한다. 각 개별 사례에서 행정 과태료 부과 여부를 결정하거나 행정 과태료 액수를 결정할 때 다음 사항을 면밀히 고려해야 한다. (a) 관련 정보처리의 성격, 범위 또는 목적을 고려한 침해의 성격, 중대성 및 기간, 그리고 영향을 받은 개인보주체의 수와 피해 정도 (b) 고의적이거나 태만한 침해 특성 (c) 개인정보주체가 입은 피해를 완화하기 위해 개인정보처리자나 수탁처리자가 취한 조치 (d) 제25조 및 제32조에 의거하여 개인정보처리자 또는 수탁처리자가 이행한 기술 및 관리적 대책을 고려한 개인정보처리자 또는 수탁처리자의 책임의 정도 (e) 개인정보처리자 또는 수탁처리자의 이전의 관련 침해건 (f) 침해를 구제하고 침해의 악영향을 완화하기 위한 감독기관과의 협력 수준 (g) 침해로 영향을 받은 개인정보의 범주 (h) 개인정보처리자 또는 수탁처리자가 침해를 통보했는지 여부 및 그런 경우 통보의 정도 등 침해 사실이 감독기관에 알려지게 된 방식 (i) 동일한 사안에 대하여 관련 개인정보처리자나 수탁처리자에 제58조(2)의 조치를 사전에 명한 경우, 해당 조치의 준수 여부 (j) 제40조에 따른 공인 행동강령 또는 제42조에 따른 공인 인증 메커니즘의 준수 (k) 침해를 통해 직접 또는 간접적으로 획득한 재정적 이익이나 회피한 손실과 같이, 해당 사례의 정황에 적용 가능한 기타의 악화 또는 완

(i) in case measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures; (j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and (k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.	화 요인
3. If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.	3. 개인정보처리자나 수탁처리자가 의도적으로 또는 부주의하여 동일하거나 연계된 정보처리 작업에 대해 본 규정의 여러 조문을 침해하는 경우, 행정 과태료의 총액은 가장 중대한 침해에 대해 명시된 금액을 초과할 수 없다.
4. Infringments of the following provisions shall, in acccordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher: (a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 42 and 43; (b) the obligations of the certification body pursuant to Articles 42 and 43; (c) the obligations of the monitoring body pursuant to Article 41(4).	4. 다음과 같은 조문의 침해는 제2항에 따라 10 000 000 유로에 이르는 행정 과태료 또는 사업체의 경우 직전 회계연도의 연간 전 세계 총 매출의 2%에 이르는 행정 과태료 중 높은 금액의 처분을 받는다. (a) 제8, 11, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 42조 및 제43조에 따른 개인정보처리자 및 수탁처리자의 의무 (b) 제42조 및 제43조에 따른 인증 기관의 의무 (c) 제41조(4)에 따른 모니터링 기관의 의무
5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher: (a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9; (b) the data subjects' rights pursuant to Articles 12 to 22; (c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49; (d) any obligations pursuant to Member State law adopted unter Chapter IX; (e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).	5. 다음과 같은 조문의 침해는 제2항에 따라 20 000 000 유로에 이르는 행정 과태료 또는 사업체의 경우 직전 회계연도의 연간 전세계 총 매출의 4%에 이르는 행정 과태료 중 높은 금액의 처분을 받는다. (a) 제5조, 제6조, 제7조 및 제9조에 따른 동의 조건을 비롯한 정보처리의 기본 원칙 (b) 제12조-제22조에 따른 개인정보주체의 권리 (c) 제44조-제49조에 따른 제3국이나 국제기구의 수령인에게로의 개인정보 이전 (d) IX장에 따라 채택된 회원국 법률에 따른 의무 (e) 제58조(2)에 따라 감독기관이 내린 명령, 또는 정보처리의 한시적 또는 확정적 제한, 또는 개인정보 이동의 중지를 준수하지 않거나 열람의 기회를 제공하지 않아 제58조(1)를 위반

6. Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in acccordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.	6. 제58조(2)에 명시된 바와 같이 감독기관의 명령 불복은 제2항에 따라 20 000 000 유로에 이르는 행정 과태료 또는 사업체의 경우 직전 회계연도의 연간 전세계 총 매출의 4%에 이르는 행정 과태료 중 높은 금액의 처분을 받는다.
7. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58(2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.	7. 각 회원국은 제58조(2)에 따른 감독기관의 시정 권한을 침해하지 아니하여 해당 회원국에 설립된 공공기관 및 기구에 행정 과태료를 부과할 수 있는지, 그리고 어느 정도의 행정 과태료를 부과할 수 있는지를 규정할 수 있다.
8. The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.	8. 본 조문에 따른 감독기관의 권한 행사는 유효한 사법 구제책 및 정당한 절차 등 유럽연합 또는 회원국 법률에 따라 적절한 절차상의 안전조치의 적용을 받는다.
9. Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. Those Member States shall notify to the Commission the provisions of their laws which they adopt pursuant to this paragraph by … [two years from the date of entry into force of this Regulation] and, without delay, any subsequent amendment law or amendment affecting them.	9. 회원국의 법제가 행정 과태료를 규정하지 않는 경우, 본 조문은 관할 감독기관이 벌금을 발의하고 관할 국가 법원이 이를 부과하며 그 같은 법적 구제책이 유효하고 감독기관이 부과하는 과태료와 동등한 효력을 갖는 방식으로 적용될 수 있다. 어떠한 경우에도 부과되는 과태료는 유효하고 비례적이며 억지력이 있어야 한다. 해당 회원국은 [본 규정의 발효일로부터 2년]까지 본 항에 따라 채택하는 자국법의 조문을 집행위원회에 통보하고, 이에 영향을 미치는 차후의 개정법이나 개정안을 지체 없이 집행위원회에 통보해야 한다.
Article 84 **Penalties**	**제84조** **처벌**
1. Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.	1. 회원국은 본 규정의 침해, 특히 제83조의 행정 과태료의 대상이 되지 않는 침해에 적용 가능한 기타 처벌에 관해 규정하고 해당 규정의 시행에 필요한 모든 조치를 취해야 한다. 그 같은 처벌은 유효하고 비례적이며 억지력이 있어야 한다.
2. Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to paragraph 1, by … [two years from the date of entry into force of this Regulation] and, without delay, any subsequent amendment affecting them.	2. 각 회원국은 [본 규정의 발효일로부터 2년]까지 제1항에 따라 채택하는 자국법의 조문을 집행위원회에 통보하고 이에 영향을 미치는 차후의 개정안을 지체 없이 집행위원회에 통보해야 한다.

CHAPTER IX PROVISIONS RELATING TO SPECIFIC PROCESSING SITUATIONS	제IX장 특정 정보처리 상황에 관한 규정
Article 85 **Processing and freedom of expression and information**	**제85조** **개인정보 처리 및 표현과 정보의 자유**
1. Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.	1. 회원국은 법률로써 본 규정에 의거한 개인정보 보호권과 언론 목적 및 학술, 예술 또는 문학적 표현 목적의 개인정보 처리 등 표현과 정보의 자유권 사이의 균형을 유지시켜야 한다.
2. For processing carried out for journalistic purposes or the purpose of academic artistic or literary expression, Member States shall provide for exemptions or derogations from Chapter II (principles), Chapter III (rights of the data subject), Chapter IV (controller and processor), Chapter V (transfer of personal data to third countries or international organisations), Chapter VI (independent supervisory authorities), Chapter VII (cooperation and consistency) and Chapter IX (specific data processing situations) if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.	2. 언론 목적이나 학술, 예술 또는 문학적 표현의 목적으로 시행되는 개인정보 처리에 대하여 회원국이 개인정보 보호권과 표현 및 정보의 자유권 사이의 균형을 유지시켜야 할 필요가 있는 경우. 제2장(원칙), 제3장(개인정보주체의 권리), 제4장(개인정보처리자 및 수탁처리자), 제5장(제3국 또는 국제기구로의 개인정보 이전), 제6장(독립적 감독기관), 제7장(협력 및 일관성), 제9장(특정 정보처리 상황)의 면제 또는 적용 일부 제외를 규정해야 한다.
3. Each Member State shall notify to the Commission the provisions of its law which it has adopted pursuant to paragraph 2 and, without delay, any subsequent amendment law or amendment affecting them.	3. 각 회원국은 제2항에 따라 채택한 자국법의 조문과 이에 영향을 미치는 차후의 개정법 또는 개정안을 지체 없이 집행위원회에 통보해야 한다.
Article 86 **Processing and public access to official documents**	**제86조** **개인정보 처리 및 공식 문서 공개**
Personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with Union or Member State law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data pursuant to this Regulation.	공공당국, 공공기관 또는 민간기관가 공익을 위해 실시하는 업무의 수행을 위해 보유하고 있는 개인정보는 본 규정에 따른 공식 문서의 일반 공개와 개인정보 보호권 사이의 균형을 유지시키기 위해 유럽연합 법률 또는 해당 공공당국이나 기관에 적용되는 회원국 법률에 의거하여 해당 기관이나 기구가 공개할 수 있다.
Article 87 **Processing of the national identification number**	**제87조** **국가 식별번호의 처리**
Member States may further determine the specific conditions for the processing of a national identification number or any other identifier of general application. In that case the national identification number or any other identifier of general application	회원국은 국가마다의 식별번호나 일반적으로 적용되는 기타 식별자의 처리에 대해 구체적인 조건을 추가로 결정할 수 있다. 그 같은 경우 국가마다의 식별번호나 일반적으로 적용되는 기타 식별자는 본 규정에 따른 개인정보주체의 권리 및 자유를 위한 적절한 안전조치가 있는 경우에 한해서만

shall be used only under appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation.	활용되어야 한다.
Article 88 **Processing in the context of employment**	**제88조** **고용 환경에서의 정보처리**
1. Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.	1. 회원국은 법률이나 단체 협약으로써 고용 환경에서 피고용인의 개인정보의 처리에 대해 특정 규정을 정할 수 있고, 특히 고용 환경에서 개인정보가 피고용인의 동의, 고용 목적, 법률이나 단체 협약이 규정한 의무 이행 등 고용 계약의 이행, 작업의 관리·계획·조직, 직장 내의 평등·다양성, 작업 중의 건강·안전을 근거로 처리되고, 개별 또는 단체적 차원에서 고용과 관련한 권리 및 혜택을 행사하기 위한 목적으로 처리되며, 고용 관계의 종결을 목적으로 처리되는 조건에 대해 규정할 수 있다.
2. Those rules shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of entreprises engaged in a joint economic activity and monitoring systems at the work place.	2. 그 같은 규정에는 특히 정보처리의 투명성과 공동 경제활동에 종사하는 사업체 또는 기업 집단 내에서 이루어지는 정보 이전, 직장에서의 모니터링 시스템과 관련하여 개인정보주체의 존엄성과 정당한 이익 및 기본권을 보호하는데 적절하고 구체적인 대책이 포함되어야 한다.
3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by … [two years from the date of entry into force of this Regulation] and, without delay, any subsequent amendment affecting them.	3. 각 회원국은 [본 규정의 발효일로부터 2년]까지 제1항에 따라 채택하는 자국법의 조문을 집행위원회에 통보하고, 이에 영향을 미치는 차후의 개정안을 지체 없이 집행위원회에 통보해야 한다.
Article 89 **Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes**	**제89조** **공익적 기록보존 목적, 과학적 또는 역사적 연구 목적, 또는 통계적 목적을 위한 처리와** **관련한 안전조치 및 적용의 일부 제외**
1. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.	1. 공익적 기록보존 목적, 과학적 또는 역사적 연구 목적, 또는 통계적 목적을 위한 처리는 개인정보주체의 권리 및 자유를 위해 본 규정에 따라 적정한 안전조치가 적용되어야 한다. 그러한 안전조치는 특히 데이터 최소화 원칙이 준수되도록 기술 및 관리적 조치를 이행해야 한다. 그러한 조치에는 가명처리 방식으로 그러한 목적들을 달성할 수 있다면 가명처리가 포함될 수 있다. 개인정보주체의 식별을 허용하지 않거나 더 이상 허용하지 않는 추가 처리를 통해 그러한 목적들을 달성될 수 있는 경우에는 그러한 방식으로 달성되어야 한다.

2. Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.	2. 개인정보가 과학적 또는 역사적 연구 목적이나 통계적 목적으로 처리되는 경우, 유럽연합 또는 회원국 법률은 본 조 제1항의 조건 및 안전조치에 따라 제15조, 제16조, 제18조 및 제21조에 규정된 권리의 적용을 일부 제외할 수 있다. 단, 그러한 권리가 그러한 특정 목적의 달성을 불가능하게 하거나 중대하게 손상시킬 것으로 예상되고, 그러한 목적을 달성하기 위하여 적용의 일부 제외가 필요한 것이어야 한다.
3. Where personal data are processed for archiving purposes in the public interest, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18, 19, 20 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.	3. 공익을 위한 유지보존의 목적으로 개인정보가 처리되는 경우, 유럽연합 또는 회원국 법률은 제15조, 제16조, 제18조, 제19조, 제20조 및 제21조에 명시되고 본 조 제1항의 조건 및 안전조치에 따른 권리로 인해 특정 목적의 달성을 불가능하게 하거나 중대하게 손상시킬 것으로 예상되고, 적용의 일부 제외가 해당 목적을 달성하기 위해 요구되는 한, 해당 권리의 적용을 일부 제외하도록 규정할 수 있다.
4. Where processing referred to in paragraphs 2 and 3 serves at the same time another purpose, the derogations shall apply only to processing for the purposes referred to in those paragraphs.	4. 제2항 및 제3항에 명시된 정보처리가 동시에 다른 목적으로 이루어지는 경우, 적용의 일부 제외는 해당 호에 명시된 목적을 가진 정보처리에만 적용되어야 한다.
Article 90 **Obligations of secrecy**	**제90조** **기밀유지의 의무**
1. Member States may adopt specific rules to set out the powers of the supervisory authorities laid down in points (e) and (f) of Article 58(1) in relation to controllers or processors that are subject, under Union or Member State law or rules established by national competent bodies, to an obligation of professional secrecy or other equivalent obligations of secrecy where this is necessary and proportionate to reconcile the right of the protection of personal data with the obligation of secrecy. Those rules shall apply only with regard to personal data which the controller or processor has received as a result ofor has obtained in an activity covered by that obligation of secrecy.	1. 회원국은 개인정보 보호권과 기밀유지 의무 사이의 균형을 유지시키기 위해 필요하고 적절한 경우, 유럽연합 법률 또는 국가 관할 기구가 정한 회원국 법률이나 규정에 따라 직업상의 기밀유지 의무 또는 이에 상응하는 기타 기밀유지의 의무가 있는 개인정보처리자나 수탁처리자와 관련하여 제58조(1)의 (e)호와 (f)호에 규정된 감독기관의 권한을 규정하는 특정 규칙(rules)들을 채택할 수 있다. 그러한 규칙은 해당 기밀유지의 의무가 적용되는 활동의 결과로 또는 활동 중에 개인정보처리자나 수탁처리자가 입수한 개인정보에 한하여 적용되어야 한다.
2. Each Member State shall notify to the Commission the rules adopted pursuant to paragraph 1, by … [two years from the date of entry into force of this Regulation] and, without delay, any subsequent amendment affecting them.	2 각 회원국은 [본 규정의 발효일로부터 2년]까지 제1항에 따라 채택하는 자국법의 조문을 집행위원회에 통보하고, 이에 영향을 미치는 차후의 개정안을 지체 없이 집행위원회에 통보해야 한다.
Article 91 **Existing data protection rules of churches and religious associations**	**제91조** **교회 및 종교 단체의 현행 정보보호 규정**
1. Where in a Member State, churches and religious associations or communities apply, at the time of entry into force of this Regulation, comprehensive rules relating to the protection of natural persons with regard to processing, such rules may	1. 본 규정이 발효되는 시점에서 회원국 내 교회 및 종교 단체나 공동체가 개인정보의 처리와 관련하여 개인의 보호에 관한 포괄적인 규정을 적용하는 경우, 그 규정이 본 규정에 부합한다면 계속 적용될 수 있다.

continue to apply, provided that they are brought into line with this Regulation.	
2. Churches and religious associations which apply comprehensive rules in accordance with paragraph 1 shall be subject to the supervision of an independent supervisory authority, which may be specific, provided that it fulfils the conditions laid down in Chapter VI of this Regulation.	2. 제1항에 따라 포괄적인 규칙을 적용하는 교회 및 종교 단체는 독립적 감독기관의 통제를 받게 되고 이는 구체적일 수 있다. 단, 이로써 본 규정의 제6장이 정한 조건이 충족되는 경우에 그러하다.
CHAPTER X **DELEGATED ACTS AND IMPLEMENTING ACTS**	**제X장** **위임법률 및 이행법률**
Article 92 **Exercise of the delegation**	**제92조** **위임의 행사**
1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.	1. 본 조문에 규정된 조건에 따라 집행위원회는 위임법률을 채택할 수 있는 권한을 부여 받는다.
2. The delegation of power referred to in Article 12(8) and Article 43(8) shall be conferred on the Commission for an indeterminate period of time from … [the date of entry into force of this Regulation].	2. 제12조(8) 및 제43조(8)에 명시된 권한의 위임은 본 규정의 발효일로부터 무기한으로 집행위원회에 부여된다.
3. The delegation of power referred to in Article 12(8) and Article 43(8) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following that of its publication in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.	3. 제12조(8) 및 제43조(8)에 명시된 권한의 위임은 유럽의회나 각료이사회에 의해 언제든지 취소될 수 있다. 취소 결정이 내려지면 그 결정에 명시된 권한의 위임은 종료된다. 결정은 유럽연합 관보에 게재된 다음 날 또는 거기에 지정된 차후의 날짜에 발효된다. 결정은 이미 발효 중인 위임법률의 유효성(효력)에는 영향을 미쳐서는 아니 된다.
4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.	4. 집행위원회는 위임법률의 채택 즉시 유럽의회와 각료이사회에 그 사실을 통보해야 한다.
5. A delegated act adopted pursuant to Article 12(8) and Article 43(8) shall enter into force only if no objection has been expressed by either the European Parliament or the Council within a period of three months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by three months at the initiative of the European Parliament or of the Council.	5. 제12조(8) 및 제43조(8)에 따라 채택된 위임법률은 유럽의회나 각료이사회가 이에 대해 통보 받은 후 3개월 이내에 이의를 표명하지 않거나, 그 기간이 만료되기 전 유럽의회와 각료이사회 양 측이 모두 이의가 없음을 집행위원회에 통보한 경우에만 발효된다.

Article 93 **Committee procedure**	**제93조** **위원회(Committee) 절차**
1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.	1. 집행위원회(Commission)는 위원회(committee)의 지원을 받아야 한다. 이 위원회는 규정서 (EU) No 182/2011의 범위에 해당하는 위원회이다.
2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.	2. 본 항을 참조하는 경우, 규정서 (EU) No 182/2011의 제5조가 적용되어야 한다.
3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.	3. 본 항을 참조하는 경우, 규정서 (EU) No 182/2011의 제5조 및 제8조가 적용되어야 한다.
CHAPTER XI **FINAL PROVISIONS**	**제XI장** **최종 규정**
Article 94 **Repeal of Directive 95/46/EC**	**제94조** **지침 95/46/EC의 폐기**
1. Directive 95/46/EC is repealed with effect from … [two years from the date of entry into force of this Regulation].	1. 지침 95/46/EC는 [본 규정의 발효일로부터 2년]에 폐기된다.
2. References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC shall be construed as references to the European Data Protection Board established by this Regulation.	2. 폐기된 지침에 대한 참조는 본 규정에 대한 참조로 해석되어야 한다. 지침 95/46/EC의 제29조가 정한 개인정보 처리와 관련된 개인보호 작업반에 대한 참조는 본 규정이 정한 유럽정보보호이사회에 대한 참조로 해석되어야 한다.
Article 95 **Relationship with Directive 2002/58/EC**	**제95조** **지침 2002/58/EC와의 관계**
This Regulation shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC.	본 규정은 유럽연합 역내의 공공 통신 분야에서 공용의 전자 통신 서비스를 제공하는 것과 관련해 개인 또는 법인이 지침 2002/58/EC에 규정된 동일한 목적의 특정 의무를 따라야 하는 사안에 대하여 그들에게 추가적 의무를 부과해서는 아니 된다.
Article 96	**제96조**

Relationship with previously concluded Agreements	이전에 체결된 협정과의 관계
International agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to … [the date of entry into force of this Regulation], and which are in accordance with Union law applicable prior to … [the date of entry into force of this Regulation], shall remain in force until amended, replaced or revoked.	본 규정의 발효일 이전에 회원국들이 제3국이나 국제기구로의 개인정보 이전과 관련해 체결하고, 본 규정의 발효일 이전에 적용 가능한 유럽연합 법률에 부합하는 국제 협정은 개정, 대체, 또는 폐지될 때까지 유효해야 한다.
Article 97 **Commission reports**	**제97조** **집행위원회 보고서**
1. By … [4 years after the date of entry into force of this Regulation] and every four years thereafter, the Commission shall submit a report on the evaluation and review of this Regulation to the European Parliament and to the Council. The reports shall be made public.	1. 집행위원회는 [본 규정의 발효 후 4년]까지, 그리고 이후 매 4년마다, 본 규정의 평가 및 검토에 관한 보고서를 유럽의회 및 각료이사회에 제출해야 한다. 보고서는 공개되어야 한다.
2. In the context of the evaluations and reviews referred to in paragraph 1, the Commission shall examine, in particular, the application and functioning of: (a) Chapter V on the transfer of personal data to third countries or international organisations with particular regard to decisions adopted pursuant to Article 45(3) of this Regulation and decisions adopted on the basis of Article 25(6) of Directive 95/46/EC; (b) Chapter VII on cooperation and consistency.	2. 제1항에 명시된 평가 및 검토를 할 때 집행위원회는 특히 다음 사항의 적용 및 기능을 면밀히 검토해야 한다. (a) 특히 본 규정의 제45조(3)에 따라 채택되는 결정 및 지침 95/46/EC의 제25조(6)을 근거로 채택되는 결정과 관련하여 제3국이나 국제기구로의 개인정보 이전에 대해 규정한 제5장 (b) 협력 및 일관성에 관한 제7장
3. For the purpose of paragraph 1, the Commission may request information from Member States and supervisory authorities.	3. 제1항의 목적을 위하여, 집행위원회는 회원국과 감독기관에 정보를 요청할 수 있다.
4. In carrying out the evaluations and reviews referred to in paragraphs 1 and 2, the Commission shall take into account the positions and findings of the European Parliament, of the Council, and of other relevant bodies or sources.	4. 집행위원회는 제1항 및 제2항의 평가와 검토를 시행할 때 유럽의회, 각료이사회 및 기타 관련 기구나 정보원의 입장 및 조사결과를 참작해야 한다.
5. The Commission shall, if necessary, submit appropriate proposals to amend this Regulation, in particular taking into account of developments in information technology and in the light of the state of progress in the information society.	5. 집행위원회는 필요한 경우 특히 정보기술의 발전과 정보사회 발전 현황을 참작하여 본 규정을 개정하는데 적정한 제안서를 제출해야 한다.
Article 98 **Review of other Union legal acts on data protection**	**제98조** **기타 유럽연합의 정보보호 법률에 대한 검토**
The Commission shall, if appropriate, submit legislative proposals with a view to amending other Union legal acts on the protection of personal data, in order to ensure uniform and consistent	집행위원회는 적절한 경우, 정보처리에 대해 균일하고 일관된 개인의 보호를 보장하고자 개인정보 보호에 대한 유럽연합의 기타 법률을 개정할 목적의 입법안을 제출해야 한다. 이는 특히 유럽연합 산하기관, 기구, 사무소

protection of natural persons with regard to processing. This shall in particular concern the rules relating to the protection of natural persons with regard to processing by Union institutions, bodies, offices and agencies and on the free movement of such data.	및 에이전시의 정보처리와 관련한 개인의 보호와 해당 개인정보의 자유로운 이동에 관한 규정에 관한 것이어야 한다.
Article 99 **Entry into force and application**	**제99조** **발효 및 적용**
1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.	1. 본 규정은 『유럽연합 관보(Official Journal of the European Union)』에 게재된 날로부터 20일 후에 발효된다.
2. It shall apply from … [two years from the date of entry into force of this Regulation].	2. 본 규정은 [본 규정의 발효 후 2년]부터 적용된다.
This Regulation shall be binding in its entirety and directly applicable in all Member States. Done at …, For the European Parliament For the Council The President The President	본 규정은 전체로서 법적 구속력을 가지며 모든 회원국들에 직접적으로 적용 가능해야 한다. 유럽의회 의장 유럽각료이사회 의장