| 발 간 등 록 번 호 |
| --- |
| 11-1079930-000026-01 |

# EU 개인정보보호법제(GDPR) 분석 및 개인정보보호법제 개선 입법수요 연구

2016. 7.21.

연구기관 : 고려대학교 산학협력단

개인정보보호위원회
Personal Information Protection Commission

이 보고서는 2016년도 개인정보보호위원회 정책연구용역으로 수행된 연구결과로서 보고서 내용은 연구자의 견해이며, 개인정보보호위원회의 공식입장과 다를 수 있습니다.

# 제 출 문

**개인정보보호위원회 위원장** 귀하

본 보고서를 『EU 개인정보보호법제(GDPR) 분석 및 개인정보보호 법제 개선 입법수요 연구』의 연구보고서로 제출합니다.

2016년 7월 21일


연 구 기 관 고려대학교 산학협력단

총괄책임자 박노형(고려대 법학전문대학원)

참여연구원 정명현(고려대 법학전문대학원)

김효권(고려대 사이버법센터)

# 요약문

## 1. 제목

EU 개인정보보호법제(GDPR) 분석 및 개인정보보호법제 개선 입법수요 연구

## 2. 연구의 배경과 목적

본 연구는 GDPR과 국내 관련 법제와의 비교 분석을 통하여 첨단 ICT환경에서 바람직한 개인정보보호 법제의 개선방향을 모색하고 입법수요를 도출하는 데 주된 목적을 둔다.

## 3. 연구의 범위

본 연구에서는 신설된 GDPR의 주요 내용과 현행 개인정보보호법의 관련 규정을 비교한다. 다음으로 빅 데이터 분석(big data analytics) 등 개인정보의 활용을 허용하고 있는 GDPR의 목적 외 처리 및 가명처리 관련 규정을 개인정보보호법과 비교·분석하고 입법방안을 모색하였다.
이러한 과정에서, 미국의 비식별정보(de-identified data) 및 일본의 익명가공정보와 같은 주요 선진국의 입법례를 함께 검토하였다.
마지막으로 GDPR의 주요 쟁점으로서 프로파일링 및 동의 규정에 대하여 별도의 장에서 검토하였다.

## 4. 연구의 내용

1) GDPR과 개인정보보호법 비교 분석

GDPR은 아동에 대한 특별한 보호의 필요성을 강조하고 투명성, 잊혀질 권리 등 관련 여러 조항에 명시적으로 언급하고 있다. 둘째, 정보주체의 권리는 개인정보보호법에서 규정된 정보주체의 권리를 모두 포함할 뿐만 아니라, 자기정보 이전에 관한 권리, 반대권 등 개인정보보호법에서 다루고 있지 않는

권리를 다루고 있다. 셋째, 국내법상 개인정보 영향평가는 공공기관을 대상이 대규모 개인정보파일의 처리하는 경우 그 위험성을 제3자인 평가기관으로 하여금 평가하도록 하는 반면, GDPR은 개인정보처리 이전에 개인정보처리자로 하여금 그러한 처리에 대한 위험성을 자체적으로 평가하도록 규정하고 있다. 평가 대상을 선정함에 있어서 산술적 기준에 근거하는 개인정보보호법과 달리, GDPR은 평가 대상이 되는 개인정보 처리의 유형을 규정하고 있으며, 평가의 결과에 따라 해당 개인정보의 처리가 위험하다고 판단되는 경우, GDPR은 사전협의 과정에서 감독당국으로 하여금 처리의 금지를 포함한 구속력있는 제재를 가할 수 있도록 규정하고 있다는 점에서 개인정보보호법의 영향평가와 차이를 보인다. 넷째, GDPR에 따른 행동강령의 제정은 특정 업종에 종사하는 개인정보처리자의 개인정보처리가 특정 상황에서 어떻게 규율될 수 있는지에 대한 자율적인 가이드라인 역할을 할 것으로 기대된다. 다섯째, GDPR은 국외이전에 대하여 구체적이고 세부적인 규정을 두어 유럽연합의 보호수준에 미치지 못하는 제3국 또는 국제기구로의 개인정보 이전을 금지하고 있다. 여섯째, GDPR에서 감독당국은 독립성이 보장된 국가기관으로 그 임무가 방대하고 권한이 막강하다. 향후 우리기업이 EU 역내 기업과 동등한 지위로 활동하기 위해서는 EU 개인정보보호 적합성 평가의 통과가 필요한바, 이를 위해서는 GDPR에서 요구하는 감독기관의 독립성과 임무와 권한을 개인정보보호위원회에 부여하여야 한다.

2) 빅데이터 분석 등 개인정보보호 활용방안

GDPR은 개인정보의 가치를 극대화하는 동시에, 정보주체의 권리를 보호하기 위해 익명처리와 가명처리를 구분하고, 재식별 가능성을 필연적으로 수반하는 가명처리정보를 개인정보로서 GDPR의 적용범위에 포섭시키는 한편 공익을 위한 기록보존, 과학 및 역사 연구, 통계 목적으로 개인정보를 처리하는 경우 예외를 인정하고 있다. 이와 달리, 미국과 일본의 개인정보보호법제는 재식별 가능성이 희박한 비식별정보 및 익명가공정보를 더 이상 개인정보로 취급하지 않는 동시에, 해당 정보가 재식별되는 것을 방지하기 위하여 재시별 금지 규정 등을 포함한 여러 관련 규정을 도입하고 있다.

빅 데이터 분석을 포함한 개인정보의 활용을 보다 폭 넓게 허용하기 위하여 GDPR을 반영하는 경우, 개인정보보호법은 가명처리정보의 목적 외 이용·제

공을 허용하는 방식으로 해석·개정될 수 있다. 이와 달리, 개인정보보호법이 미국 및 일본의 법제를 반영하는 경우 - 즉, 비식별 처리된 개인정보를 더 이상 개인정보로 취급하지 않는 경우 - 학술연구 또는 통계목적 뿐만 아니라, 다른 목적에 근거한 비식별 정보의 활용 역시 허용될 수 있다.

3) 프로파일링과 동의 관련 규정 검토

개인정보보호법과 달리, GDPR은 빅 데이터 분석과 불가분의 관계에 있는 프로파일링을 포함한 대규모 자동처리 방식에 따른 개인정보의 처리를 별도로 규율하고 있다. 이에 따라 프로파일링을 시행하는 개인정보처리자는 반드시 해당 처리의 위험성을 사전에 예측하기 위하여 개인정보 영향평가를 시행하여야만 하며, 정보주체는 인간의 개입이 전혀 존재하지 않는 자동화된 방식의 개인정보처리 결과에 종속되지 않을 권리를 가진다. 또한 동의와 관련하여, 일반적으로 정보주체의 동의는 개인정보 수집을 포함한 처리를 적법하게 만드는 기본적인 법적 근거이다. 그러나 정보주체의 동의는 개인정보 처리를 위한 다양한 법적 근거 중의 하나에 불과하며, 이러한 동의는 언제든지 철회될 수 있다는 점에서 가장 안전한 또는 안정된 법적 근거가 될 수 없다. 그럼에도 불구하고, 정보주체의 동의가 자신의 개인정보 처리를 통제하는데 가장 좋은 수단이라는 사실에는 이견이 있을 수 없다. 정보주체의 동의에 근거하여 그의 개인정보를 처리하는 개인정보처리자는 동의가 주어지는 방식과 관련 문서가 GDPR의 관련 규정에 비추어 적절한지 유의하여야 하며, 특히 동의가 주어진 사실에 대한 입증책임이 개인정보처리자가 있음을 유의하여야 할 것이다. 동의에 근거한 개인정보의 처리가 어려운 경우, 특히 사업자인 개인정보처리자는 GDPR 제6(1)(f)에 규정된 개인정보처리자 또는 제3자의 정당한 이익에 근거한 개인정보 처리에 보다 더 큰 관심을 가질 것으로 보인다.

## 5. 기대효과

본 연구 결과는 EU GDPR와 국내 법제를 비교 분석하고 우리 법제의 개선방향을 제시함으로써 빅데이터 등 기술 발전 대응 및 국제적 상호운용성을 갖추기 위한 자료로 활용할 수 있다.

# < 목 차 >

# I. 서 론

## 1. 연구의 배경과 목적

최근 유럽연합은 개인정보보호의 권리 신장과 디지털단일시장에서 개인정보의 자유로운 이동을 원활하게 하는 내용의 '일반개인정보보호규칙 (General Data Protection Regulation, 이하 GDPR)'을 채택하였다. GDPR은 2018년 5월 28일자로 발효하며, 기존 1995년 개인정보보호지침(Data Protection Directive 95/46/ec)을 대체하게 된다. GDPR은 유럽연합의 입법 형식 가운데 규칙(regulation)의 형식을 취하고 있으므로, 모든 회원국에서 직접적으로 적용된다. 1995년 개인정보보호지침 이후 21년 만에 채택된 GDPR은 그 동안의 인터넷 등 과학기술적 발전을 적극적으로 반영하였다. 특히 정보주체(data subject)를 보다 더 보호하고 개인정보처리자(data controller)와 수탁처리자(data processor)의 책임을 강화하는 동시에, 빅 데이터 분석을 포함한 디지털경제 활성화를 위하여 사업자인 개인정보처리자의 개인정보 활용의 편의를 증대함으로써, 개인정보보호와 개인정보의 활용 사이의 균형을 유지하려 하고 있다.[1] 본 연구를 통하여 EU GDPR과 국내 개인정보보호법제를 비교·분석하고, 정보화 시대에 정보주체의 권리를 보호하는 한편 개인정보의 활용을 통한 경제적 가치를 창출하기 위한 입법방안을 모색하고자 한다.

## 2. 연구의 범위와 방법

본 연구는 GDPR과 국내 관련 법제와의 비교 분석을 통하여 첨단 ICT환경에서 바람직한 개인정보보호 법제의 개선방향을 모색하고 입법수요를 도출하는 데 주된 목적을 둔다. 이를 위하여 이하에서는 신설된 GDPR의 주요 내용과 현행 개인정보보호법의 관련 규정을 비교한다. 다음으로 빅 데이터

1) GDPR에서 제4조 7항 및 8항에 따라 'controller'는 개인정보 처리의 목적과 방법을 단독 또는 제 3자와 공동으로 결정하는 자연인 또는 법인, 공공 기관, 관청, 기타 단체를 의미하며, 'processor'는 이러한 'controller'를 대신하여 개인정보를 처리하는 자이다. GDPR에서 규정하는 'data controller'와 'data processor'는 용어의 통상적 의미만을 고려하였을 때, 각각 '개인정보관리자'와 '개인정보처리자'로 서술되는 것이 타당하다. 그러나 현행 개인정보보호법은 '개인정보처리자'를 "업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인"으로(제2조 5항), '수탁자'를 "개인정보 처리 업무를 위탁받아 처리하는 자"로 정의하는 바(제26조 2항), 개인정보처리자는 'data controller', 수탁자는 'data processor'와 그 개념이 유사하다. 이하에서는 용어의 중복과 혼동을 피하기 위하여, GDPR에서 규정하고 있는 'data controller'를 '개인정보처리자', 'data processor'를 '수탁처리자'로 서술한다.

분석(big data analytics) 등 개인정보의 활용을 허용하고 있는 GDPR의 목적 외 처리 및 가명처리 관련 규정을 개인정보보호법과 비교·분석하여, 정보주체의 권리를 보호하는 동시에, 개인정보의 활용을 통한 경제적 가치 창출을 도모하기 위한 균형 잡힌 입법방안을 모색한다. 이러한 과정에서, 미국의 비식별정보(de-identified data) 및 일본의 익명가공정보와 같은 주요 선진국의 입법례를 함께 논의한다. 마지막으로 GDPR의 주요 쟁점으로서 프로파일링 및 동의 규정에 대하여 별도의 장에서 검토한다.

# II. GDPR과 개인정보보호법 비교분석

## 1. 아동에 대한 특별 규정

GDPR과 개인정보보호법은 아동의 동의를 받는 방식에 대하여 규정하고 있다. GDPR 제8조 1항은 정보사회서비스(information society service)를 아동에게 직접 제공하는 경우에 대하여, 16세 미만의 아동에 대하여 후견인(holder of parental responsibility)의 동의 또는 승인을 요구하고 있다. 회원국은 16세 미만으로 지정된 아동의 나이를 법으로 낮추어 규정할 수 있으나, 그러한 경우라 하더라도 아동의 나이를 13세 미만으로 규정할 수 없다.[2)]

개인정보보호법 제22조 5항은 개인정보처리자로 하여금 만 14세 미만 아동의 개인정보를 처리하기 위하여 동의를 받아야 하는 경우, 해당 아동의 법정대리인의 동의를 받을 것을 요구하고 있으며, 이러한 경우 법정대리인의 동의를 받기 위하여 필요한 최소한의 정보는 해당 아동으로부터 직접 수집할 수 있음을 규정하고 있다.[3)]

아동의 동의를 받는 방식만을 규정한 개인정보보호법과 달리, GDPR은 아동에 대한 특별한 보호(specific protection)의 필요성을 명시적으로 언급하고 있다. 이처럼 아동에게 특별한 보호가 부여되는 이유는 아동은 자신의 개인

2) GDPR Art. 8. 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.

3) 개인정보보호법 제22조 5항.

정보 처리가 어떠한 위험을 내포하는지, 어떠한 결과를 야기하는지에 대하여 충분히 숙지하기 어렵기 때문이다.[4] 이러한 보호의 필요성에 근거하여 GDPR은 다음의 여러 관련 조항을 통하여 아동을 보호하고 있다.

먼저, 투명성 원칙(principle of transparency)을 규정한 GDPR 제12조는 개인정보처리자로 하여금 정보주체에 대한 고지, 정보주체의 권리를 행사하는 과정에서의 의견교환에 있어서 정보주체의 쉬운 이해를 위하여 쉽고 분명한 언어를 사용할 것을 요구하고 있는 바, 이러한 투명성 원칙은 특히 정보주체가 아동인 경우에 특별히 요구된다.[5]

다음으로, 잊혀질 권리를 규정하고 있는 GDPR 제17조 1항(f)는 SNS와 같은 정보사회서비스 이용 과정에서 아동의 동의에 근거하여 수집된 개인정보에 대하여, 정보주체로 하여금 해당 개인정보를 개인정보처리자에게 삭제할 것을 요구할 수 있도록 규정하고 있다.[6] 이처럼 아동의 동의하에 수집된 개인정보를 삭제할 것을 요구하는 잊혀질 권리는 해당 권리를 행사하는 정보주체가 여전히 아동인지 혹은 성인이 되었는지를 구분하지 않는다.[7] 투명성 원칙, 잊혀질 권리 이외에도 아동에 대한 특별한 보호는 행동강령을 규정한 제40조, 감독당국의 임무를 규정한 제57조 등에서 명시적으로 언급되어 있다.[8]

---

4) GDPR Recital (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.

5) GDPR Art. 12. 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.

6) GDPR Art. 17 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: (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

7) GDPR Recital (65) (...) 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.

8) GDPR Art. 40 2. Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to: (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; Art. 57 1. Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory: (b) promote public awareness and understanding of the risks, rules, safeguards and rights in

## 2. 정보주체의 권리[9)]

### 2.1. 정보를 제공받을 권리

GDPR은 개인정보를 수집함에 있어서 어떠한 내용의 정보(information)가 정보주체에게 고지되어야 하는지를 정보주체의 권리로서 접근하고 있다. 이는 개인정보보호법이 고지의무를 정보주체의 권리가 아닌 개인정보처리자의 의무로서 접근하는 방식과 다르다. 먼저, 정보주체로부터 개인정보가 수집되는 경우를 규정한 GDPR 제13조에 따라 정보주체는 ① 개인정보처리자의 기관명과 연락처, ② 개인정보보호책임자(data protection officer)의 세부연락처, ③ 개인정보 처리의 목적·근거, ④ 개인정보처리자의 정당한 이익(legitimate interests), ⑤ 수령인(recipient) ⑥ 국외이전이 발생하는 경우 적합성 평가 등 국외이전의 근거를 통보받을 권리를 가진다.[10)] 이와 더불어, 개인정보처리자는 개인정보를 수집함에 있어서 공정하고 투명한 처리를 보장하기 위하여 다음의 6가지 정보를 추가적으로 제공하여야만 한다. (① 저장 기간, ② 접근·정정·삭제·처리제한·거부·이동권이 있다는 사실, ③ 동의철회권, ④ 이의제기권, ⑤ 개인정보 제공이 법 또는 계약상 요구 또는 강제되는지 여부와 제공하지 않을 경우 예상되는 결과, ⑥ 프로파일링을 포함한 자동의사결정의 존재여부와 해당 논리구조에 있어 유의미한 정보 및 해당 처리의 중요성·예상되는 결과)[11)] 또한 목적 외로 개인정보를 처리하는 경우에도 개인정보처리자는 그 처리 목적과 상기 추가 정보를 정보주체에게 제공해야 한다.[12)]

다음으로, GDPR 제14조에 따라 정보주체 이외로부터 개인정보를 수집하는 경우에도 개인정보처리자는 상기 제13조에 따른 정보를 제공하여야만 한다. 이와 달리, 개인정보보호법 제20조는 정보주체 이외로부터 개인정보를 처리

---

relation to processing. Activities addressed specifically to children shall receive specific attention.

9) GDPR 제21조에서 규정하고 있는 자동화된 처리방식에 따른 의사결정에 종속되지 않을 권리는 개별적으로 후술한다.

10) GDPR Art. 13. 1.

11) GDPR Art. 13. 2.

12) GDPR Art. 13. 3.

하는 경우, “정보주체의 요구”가 있는 경우에 한하여, ① 수집출처, ② 처리목적, ③ 처리정지요구권이 있다는 사실을 정보주체에게 고지하도록 하고 있는 한편 예외적으로 대통령령으로 정하는 기준에 해당하는 개인정보처리자가 정보주체 이외로부터 개인정보를 수집하여 처리하는 때에는 정보주체에게 수집 출처·처리 목적 등을 고지하도록 하고 있다. [13] 다시 말해, 정보주체 이외로부터 개인정보가 수집되는 경우, GDPR은 정보주체의 요구와 무관하게 개인정보처리자로 하여금 고지의무를 부여하는 것과 달리, 개인정보보호법은 원칙적으로 그러한 요구가 있는 경우에 한하여 고지의무가 부여된다는 차이점이 있다.

다만, GDPR 제14조는 제13조와 달리 ① 정보주체가 이미 위 사항들을 보유하고 있는 경우, ② 위 사항들을 제공하는 것이 불가능한 것으로 입증되거나 과도한(disproportionate) 노력을 요하는 경우, ③ 수집 또는 공개가 명확히 법률에 규정되어 있는 경우, ④ 법률에 따른 업무상 기밀 유지가 필요한 경우에 정보주체의 정보를 제공받을 권리가 제한될 수 있음을 규정하고 있다.[14]

개인정보보호법은 개인정보처리자의 고지의무를 개인정보의 처리 유형 -수집과 제공 -에 따라 그 내용을 각각 달리하고 있다. 수집의 경우, 개인정보처리자는 ① 개인정보의 수집·이용 목적, ② 수집하려는 개인정보의 항목, ③ 개인정보의 보유 및 이용 기간, ④ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용을 정보주체에게 고지하여야 한다.[15] GDPR과 달리, 상기 고지내용에는 개인정보의 제3자 제공에 관한 사항, 국외이전과 관한 사항, 정보주체의 권리 등이 포함되어 있지 않다. 국외이전을 포함한 개인정보 제공의 경우, 개인정보보호법은 개인정보처리자로 하여금 ① 제공받는 자, ② 제공 목적, ③ 제공하는 개인정보 항목, ④ 보유기간, ⑤ 동의 거부권이 있다는 사실 및 거부에 따른 불이익을 고지하도록 규정하고 있다.[16]

## 2.2. 접근권 (right of access)

13) 개인정보보호법 제20조 1항, 2항, 3항, 4항
14) GDPR Art. 14. 3.
15) 개인정보보호법 제15조 2항.
16) 개인정보보호법 제17조 2항, 3항, 제18조 2항.

GDPR 제15조에 따라 정보주체는 자신의 개인정보 처리의 유무를 확인하고 개인정보 사본을 획득할 수 있으며, 해당 개인정보 처리에 대한 관련 정보를 제공받을 수 있는 권리를 가진다. 이러한 접근권을 보장하기 위하여 개인정보처리자는 정보주체에게 무료로 사본을 제공해야한다. 접근권에 따라 정보주체가 획득할 수 있는 개인정보 처리에 관한 관련 정보에는 ① 처리 목적, ② 개인정보의 유형, ③ 제공받는 자, ④ 저장 기간, ⑤ 정정·삭제·처리제한·처리반대권의 존재사실, ⑥ 감독당국에 이의를 제기할 수 있는 권리, ⑦ 정보주체 이외로부터 수집된 개인정보의 경우, 그에 대한 출처, ⑧ 프로파일링과 관련된 사항이 존재한다.[17] 또한 국외이전의 경우, 정보주체는 적합성 결정, 구속력 있는 기업규칙 등 적절한 안전장치의 여부에 대한 정보에 대한 접근을 가진다.[18] 접근권의 행사를 통하여 정보주체는 자신의 개인정보 처리 현황을 파악할 수 있으므로, 동 권리는 이하에서 규정되는 개인정보 정정·삭제·제한·이동·처리반대를 요구하기 위한 선결적 권리에 해당한다 할 것이다.

GDPR의 접근권과 유사한 규정으로 개인정보보호법 제35조는 정보주체의 열람권을 규정하고 있다. 이에 따라 정보주체는 개인정보처리자가 처리하는 자신의 개인정보에 대한 열람을 요구할 수 있으며, 개인정보처리자가 공공기관인 경우, 해당 공공기관뿐만 아니라 행정자치부 장관을 통하여 열람을 요구할 수도 있다.[19] 동법 시행령 제41조에 따라 정보주체가 열람가능한 정보로는 ① 개인정보의 항목 및 내용, ② 수집 목적, ③ 보유 기간, ④ 제3자 제공 현황, ⑤ 동의 사실 및 내용이 존재한다.[20] 시행령 제41조에 따른 열람정보가 한정적인지 예시적인지는 분명하지 않으나, 이를 한정된 정보로 해석하는 경우, 개인정보보호법에서 규정하는 열람권은 GDPR의 접근권보다 그 범위가 좁다 할 것이다. 또한 동 법률 제4항에 따라 개인정보처리자는① 법률에 따라 열람이 금지되거나 제한되는 경우, ② 다른 사람의 생명·신체를 해할 우려가 있거나 재산 등 이익을 부당하게 침해할 우려가 있는 경우, ③ 공공기관이 조세, 학교성적평가·입학자선발, 학력·기능·채용시험, 자격심사, 보상금·급부금산정, 법률에 따른 감사·조사 업무를 수행할 때 중대한 지장을 초래하는 경우에 정보주체의 개인정보 열람을 제한하거나 거절할 수 있다. 여기에서 주목할 점은 - 열람권의 예외사유에서 확인되는 바와 같이 - 개인

17) GDPR Art. 15. 1.
18) GDPR Art. 15. 2.
19) 개인정보보호법 제35조 1항, 2항.
20) 개인정보보호법 시행령 제41조 1항.

정보보호법은 제5장에서 정보주체의 권리에 대한 예외사유를 관련 조항에서 개별적으로 규정하는 반면, GDPR은 제3장 제12조 내지 제22조에서 일련의 권리를 규정하고, 동장 제23조에서 정보주체의 권리에 대한 일반적인 예외사유를 포괄적으로 규정하고 있다는 점이다. 이러한 맥락에서 GDPR에서 규정하는 접근권은 - 동 규정에서 규율하는 다른 정보주체의 권리와 마찬가지로 -제15조가 아닌 제23조의 예외사유에 근거하여 제한된다.

### 2.3. 정정권 (Right to rectification) 및 삭제권 (Right to erasure)

GDPR 제16조는 정보주체로 하여금 자신의 부정확한 정보를 정정하도록 개인정보처리자에게 요구할 수 있는 권리를 규정하고 있다. 동 권리의 행사를 위하여 정보주체는 개인정보 처리 목적을 고려하여 개인정보처리자에게 보충 설명을 할 수 있다.[21]

또한 GDPR 제17조에 따라 정보주체는 과도한 지연 없이 자신에 관한 개인정보를 삭제할 수 있는 권리, 삭제를 요청할 수 있는 권리를 가진다. 동 조항에 따라 개인정보처리자는 ① 개인정보가 불필요하게 된 경우, ② 정보주체가 동의를 철회한 경우, ③ 정보주체가 GDPR 제21조에 근거하여 개인정보 처리에 반대한 경우, ④ 개인정보가 부적법하게 처리된 경우, ⑤ 법률이 삭제하도록 한 경우에 해당 개인정보를 삭제해야 하는 의무를 가진다.[22] 특히, 제17조 1항 (f)는 정보사회서비스(information society service)[23] 제공과 관련되어 개인정보가 미성년자의 동의에 근거하여 수집된 경우에 정보주체로 하여금 잊혀질 권리(right to be forgotten)를 부여하고 있다. 이는 SNS 등 정보통신서비스를 이용하는 과정에서, 미성년자인 정보주체가 당시 개인정보처리와 관련된 위험을 충분히 인지하지 못한 경우를 고려한 것이다. 또한 삭제권 및 잊혀질 권리에 따라 정보주체가 자신의 개인정보에 대한 삭제를 요청한 상황에서 해당 정보가 인터넷 등을 통하여 공개된 경우, GDPR은 개인정보처리자로 하여금 활용 가능한 기술과 그 비용을 고려하여 해당 정보를 처리하는 또 다른 개인정보처리자에게 정보주체의 삭제 요청이 있었다

21) GDPR Art. 16.
22) GDPR Art. 17. 1.
23) 정보사회서비스(Information Society Service)란 서비스를 제공받는 사람의 요청으로 정보의 처리 및 저장을 위한 전자장비를 사용하여 제공되는 상업적인 서비스 일체로서 정보통신망법에 따른 정보통신서비스와 유사한 개념이다.

는 사실을 통지하기 위하여 합리적인 절차(reasonable steps)를 취해야 한다.[24]

이와 유사하게, 개인정보보호법 제36조에 따라 정보주체는, 해당 개인정보가 법령상 수집대상인 경우를 제외하고, 자신의 개인정보에 대한 정정 또는 삭제를 요구할 수 있다.[25] 동 조항에 따라 개인정보처리자는 정정 또는 삭제요구를 받은 때에는 10일 이내에 필요한 조치를 한 후 그 결과를 정보주체에게 알려야 하며, 삭제의 경우, 복구 또는 재생되지 않도록 조치하여야 하고, 법령상 수집대상으로 삭제할 수 없는 경우에는 지체 없이 그 내용을 정보주체에게 알려야 한다. 개인정보보호법 제36조는 GDPR 제16조 및 제17조와 비교하여 다음과 같은 차이를 보인다. 첫째, GDPR과 달리, 개인정보보호법에 따른 개인정보의 정정 또는 삭제는 동법 제35조에 따른 정보주체의 열람권 행사를 선결적으로 요구한다. 둘째, GDPR은 정정권 및 삭제권을 개별 조항에서 구체적으로 규율하고 있는 반면, 개인정보보호법은 그러하지 못하다. 예를 들어, GDPR은 정보주체가 삭제권을 행사할 수 있는 경우를 구체적으로 제시하고, 이러한 상황에서 개인정보의 삭제는 정보주체의 권리인 동시에 개인정보처리자의 의무가 된다는 점을 명시하고 있다. 이와 달리, 개인정보보호법은 정보주체의 요구가 있는 경우에 개인정보처리자로 하여금 “정정·삭제 등 필요한 조치”를 취할 것을 규정하는 바, “등”이라는 용어에 따라 삭제의 요구가 반드시 삭제조치로 귀결되지 않는 상황이 존재할 수 있다.[26] 셋째, GDPR과 달리 개인정보보호법은 잊혀질 권리를 규정하고 있지 않다. 마지막으로 넷째, GDPR과 달리, 개인정보가 이미 인터넷 등을 통하여 공개되거나 배포된 경우와 같이, 개인정보처리자가 자신의 권한·통제 밖에 놓여있는 개인정보에 대하여 어떠한 조치를 취해야만 하는지에 대하여 개인정보보호법은 규율하고 있지 않다.

## 2.4. 처리제한권 (Right to restriction of processing)

GDPR 제18조에 따라 정보주체는 자신의 개인정보에 대한 제3자 또는 대중의 접근을 금지할 것을 요구하는 권리를 가진다. 처리제한권(Right to restriction of processing)은 ① 정보주체가 자신의 개인정보에 대한 정확성에 의문을 제기한 경우, ② 처리가 불법적이고(unlawful) 정보주체가 해당

24) GDPR Art. 17. 2.
25) 개인정보보호법 제36조.
26) 개인정보보호법 제36조 2항.

정보의 삭제를 요구하는 대신 해당 정보의 이용 금지를 요청한 경우, ③ 개인정보가 더 이상 처리 목적에 근거하여 필요한 경우가 아니나, 정보주체의 법적쟁송을 위해 해당 정보가 필요한 경우, ④ 정보주체가 제21조에 따라 처리를 반대한 경우에 행사될 수 있다.[27] 이러한 경우 개인정보처리자는 해당 정보를 보유하는 것은 허용되는 반면, 그러한 정보를 제3자 또는 대중이 접근할 수 없도록 기술적 조치를 취하여야 한다.

또한 정보주체에 의하여 처리가 제한된 경우, 개인정보처리자는 ① 본인의 동의가 있는 경우, ② 법적쟁송을 위한 경우, ③ 다른 사람의 권리보호를 위한 경우, ④ 중대한 공익을 위한 경우에 한하여 해당 개인정보를 처리할 수 있으며,[28] 이러한 처리제한이 해제되는 경우 정보주체는 사전에 그러한 사실을 통보받아야 한다.[29]

GDPR의 처리제한권과 유사하게, 개인정보보호법 제37조는 처리정지권을 규정하고 있으며, 이에 따라 정보주체는 개인정보처리자에게 자신의 개인정보 처리의 정지를 요구할 수 있다.[30] 그러나 제7조 1항 단서에 따라 공공기관에 보유하고 있는 개인정보는 동 법 제32조에 따라 “등록 대상이 되는 개인정보파일”에 대하여만 처리의 정지를 요구할 수 있으므로, 동 조 2항에 따라 등록 대상이 되지 않는 공공기관의 국가안전, 외교상 비밀, 범죄수사, 공소제기, 형 집행, 조세·관세 조사, 공공기관 내부업무처리, 법령상 비밀과 관련된 개인정보는 처리의 정지를 요구할 수 없다.[31]

또한 개인정보보호법 제37조 2항에 따라 다음의 4가지 경우에는 정보주체의 처리정지권은 인정되지 않는다. (① 법률 규정이 있거나 법령상 의무 준수를 위해 불가피한 경우, ② 다른 사람의 생명·신체를 해할 우려가 있거나 재산 등 이익을 부당하게 침해할 우려가 있는 경우, ③ 공공기관이 법률상 소관업

27) GDPR Art. 18. 1.
28) GDPR Art. 18. 2.
29) GDPR Art. 18. 3.
30) 개인정보보호법 제37조.
31) 제32조(개인정보파일의 등록 및 공개) ② 다음 각 호의 어느 하나에 해당하는 개인정보파일에 대하여는 제1항을 적용하지 아니한다. 1. 국가 안전, 외교상 비밀, 그 밖에 국가의 중대한 이익에 관한 사항을 기록한 개인정보파일 2. 범죄의 수사, 공소의 제기 및 유지, 형 및 감호의 집행, 교정처분, 보호처분, 보안관찰처분과 출입국관리에 관한 사항을 기록한 개인정보파일 3. 「조세범처벌법」에 따른 범칙행위 조사 및 「관세법」에 따른 범칙행위 조사에 관한 사항을 기록한 개인정보파일 4. 공공기관의 내부적 업무처리만을 위하여 사용되는 개인정보파일 5. 다른 법령에 따라 비밀로 분류된 개인정보파일

무를 수행할 수 없는 경우, ④ 서비스 제공 등 계약이행이 곤란한 경우로서 정보주체가 계약해지 의사를 명확하게 밝히지 아니한 경우)

이상을 요약하면, GDPR은 어떠한 경우에 정보주체가 처리제한권을 행사할 수 있는지에 대하여 구체적인 요건과 절차를 규정하고 있는 반면, 개인정보보호법은 처리정지권의 행사에 대한 세부적인 규정을 마련하고 있지 않다. 또한 GDPR은 정보주체의 동의, 정보주체를 위한 법적쟁송 등 정보주체의 관점에서 처리제한에 대한 예외사유를 규정하고 있는 반면, 개인정보보호법에 따른 처리정지의 예외는 공익을 위한 목적에만 국한되고 있음을 알 수 있다.[32] 이러한 맥락에서, 개인정보처리 정지 또는 제한과 관련하여, 개인정보보호법은 GDPR과 동일한 보호수준을 구비하고 있다고 볼 수 없다.

## 2.5. 정정·삭제·제한에 있어서 통보를 받을 권리

GDPR은 개인정보처리자로 하여금 그러한 통보가 불가능하거나 과도한 노력(disproportionate effort)을 요구하는 경우가 아닌 한, 개인정보를 제공받은 수령인(recipient)[33]에게 해당 개인정보가 정정·삭제·처리제한 되었다는 사실을 알려야 한다.[34] 또한 정보주체가 요구하는 경우 개인정보처리자는 개인정보가 공개된 수령인에 대한 정보를 정보주체에게 알려야 한다. 다시 말해, GDPR은 개인정보처리자로 하여금 개인정보의 정정·삭제·처리제한의 의무를 부여하는 것과는 별개로, 개인정보가 수령인에게 이미 제공되어 자신의 통제 또는 권한을 벗어난 경우에도, 수령인에게 해당 정보의 정정·삭제·처리제한의 사실에 대한 통보의무를 부여하고 있는 것이다. 개인정보보호법에는 이와 유사한 규정이 존재하지 않는다. 따라서 정보주체의 요구가 있는 경우, 개인정보처리자는 해당 개인정보를 정정·삭제·처리정지 해야 할 의무만을 가질 뿐, 그러한 요구가 발생하기 전에 개인정보를 이미 제공받은 제3자에게 해당 정보의 정정·삭제·처리정지 등의 사실을 통보할 의무를 가지지 않는다.

32) GDPR 역시 이처럼 국가안보, 공공질서와 같은 공익을 위한 목적에 따라 처리제한권이 제한될 수 있으나, 이러한 정보주체 권리 행사의 예외는 GDPR 제23조를 통하여 포괄적으로 규율되고 있다.
33) GDPR Art. 4 (9). 수령인이란 제3자 여부를 불문하고 개인정보를 제공 받는 자연인이나 법인, 공공기관, 기구, 기타 기구를 의미한다.
34) GDPR Art. 19.

## 2.6. 자기정보 이전에 관한 권리 (Right to data portability)

GDPR 제20조에 따라 정보주체는 자신이 개인정보처리자에게 제공한 개인정보를 체계화되고, 일반적으로 사용되며, 기계로 판독가능한 형태(structured, commonly used and machine-readable format)로 수령할 권리가 있고, 이들 개인정보를 종래의 개인정보처리자에게서 다른 개인정보처리자에게로 전송할 권리를 가진다.[35] 이 때 처리는 제6조 1항 (a)에 따라 정보주체의 동의 또는 제6조 1항 (b)에 따라 계약조건의 수행에 의거하거나, 민감정보의 경우 제9조 2항 (a)에 따라 정보주체의 명시적인 동의에 의거한 것이어야 하며, 처리가 자동화된 수단(automated means)에 의해 수행되는 경우이어야 한다.[36] 정보주체는 개인정보 이동에 관한 권리를 행사함에 있어 기술적으로 가능한 경우, 개인정보처리자로 하여금 자신의 개인정보를 다른 개인정보처리자에게 직접 전송할 것을 요청할 권리가 있다.[37] 이러한 권리는 정보주체가 갖는 GDPR 제17조의 삭제권을 저해하지 않으며, 공익 목적으로 수행되는 업무나 개인정보처리자에게 부여된 공적 권한의 행사를 위해 수행될 필요가 있는 처리에는 적용되지 않는다.[38] 또한 동 권리의 행사로 인하여 다른 사람들의 권리와 자유에 부정적인 영향을 초래해서는 안 된다.[39]

자기정보 이전에 관한 권리는 GDPR이 빅데이터의 활성화 동향에 맞추어 정보주체에게 온라인 서비스에 대한 선택권을 확대하기 위하여 신설한 조항으로, 1995년 개인정보보호지침에는 없던 개념이다. 동 권리는 개인이 종전

---

35) GDPR Art. 20. 1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where: (a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and (b) the processing is carried out by automated means. 2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible. 3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. 4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

36) GDPR Art. 20.1.

37) GDPR Art. 20.2.

38) GDPR Art. 20.3.

39) GDPR Art. 20.4.

의 서비스제공자에 의해 수집되고 보관되어 왔던 자신의 개인정보를 새로운 사업자를 선택하여 이전시킬 수 있게 함으로써 개인정보에 관한 정보주체의 통제 권한을 증대시키고, 스타트업기업과 소규모업체에게는 디지털시장에서 대기업에게 선점된 개인정보시장(data market)에 접근할 수 있는 기회를 제공함으로써 기업 간 경쟁과 혁신을 증진시킬 것으로 기대되고 있다.

자기정보 이전에 관한 권리와 관련하여 해설전문 68항에서는 제20조의 '체계화되고, 일반적으로 사용되며, 기계로 판독가능한 형태' 이외에 '상호운용가능한'(interoperable) 형태를 추가하여 설명하고 있는데, 이는 GDPR 초안에서 유지되어 왔던 문안이다. 이에 따라 개인정보처리자는 개인정보 이동을 가능하게 하는 상호운용가능한 형태를 개발할 것이 권장된다.[40] 그러나 동 조항이 개인정보처리자에게 기술적으로 호환가능한 처리시스템을 도입하거나 유지할 의무를 부담시키는 것은 아니다. 기업들은 자사에서 사용하는 개인정보의 형태(format)를 확인하고, 다른 서비스 제공자에게 쉽게 이전할 수 있는지 여부를 검토하여야 한다. 그러나 고정된 소비자를 확보할 수 없는 디지털 시장에서 개인정보처리자에게 개인정보 이전을 강제하는 것은 과도한 비용과 노력을 요구할 수도 있다는 우려도 제기되고 있다. 또한 보건산업과 같은 특정 산업에서는 수행 중인 연구 또는 서비스의 지속성에 단절을 가져올 우려가 있고, 여러 정보주체가 관련된 개인정보를 이전하는 경우에는 개인정보의 이전에 동의하지 않는 다른 정보주체의 권리와 자유에 관한 문제들이 발생할 수 있다.[41]

이 권리는 그 본질상 개인정보처리자가 공익적 의무를 수행하기 위하여 처리하는 경우에는 행사될 수 없다. 즉 개인정보처리자가 법적 의무를 준수하기 위하여 개인정보 처리가 필요한 경우, 또는 공익 목적 또는 관리자에게 부여된 공적 임무 수행을 위하여 개인정보를 처리하는 경우에는 적용되지 않는다.

하나 이상의 정보주체가 관련된 개인정보집합물의 경우, 개인정보 수령의 권리 행사를 위하여 다른 정보주체의 권리와 자유를 침해해서는 안 된다. 또한 동 권리는 GDPR에서 규정하는 정보주체의 개인정보 삭제권 및 그 권리

40) GDPR Recital (68).
41) EU Data Protection Reform: Where are we - and what can you do to prepare?, Olswang LLP (2014.12.2.), p. 14.

의 제한을 방해하지 않는다. 특히 정보주체가 계약 이행을 위하여 제공한 개인정보에 관해서는, 이전권을 행사하더라도 그 개인정보가 계약 이행을 위하여 여전히 필요한 범위 내에서 정보주체에 관한 개인정보의 삭제를 암시하는 것은 아니다.[42] 개인정보처리자가 추후 발생할 수 있는 개인정보의 이동 요청에 합치하기 위하여 더 이상 필요하지 않은 데이터를 보관해서는 안 되는지 여부는 동 조항에서 명시하고 있지 않으며, 이후 명확하게 할 필요가 있다.[43]

우리나라 개인정보보호법은 제27조에서 개인정보처리자가 영업의 양도 등에 따른 개인정보 이전을 정보주체에게 고지할 의무와 개인정보를 이전받은 처리자의 이용범위에 대하여 규정하고 있으며, 개인정보의 이전 또는 이동에 대한 정보주체의 권리는 규정되어 있지 않다.

## 2.7. 반대권 (Right to object)

GDPR 제21조에 따라 정보주체는 자신의 개인정보 처리를 반대할 수 있는 권리를 가진다. 반대권은 크게 세 가지 유형으로 분류될 수 있다. 첫째, 개인정보처리자가 공익 또는 공적권한을 수행하거나 개인정보처리자의 정당한 이익을 위하여 개인정보를 처리하는 경우(프로파일링 포함), 정보주체는 자신의 특수한 상황(particular situation)에 근거하여 언제든지 해당 처리를 반대할 권리를 가진다. 이 경우 개인정보처리자는 해당 개인정보를 처리하는 것이 정보주체의 이익, 권리 및 자유의 보장보다 우월하다는 설득력 있는 정당한 근거(compelling legitimate grounds)를 입증하지 않는 한, 더 이상 해당 개인정보를 처리할 수 없다.[44] 둘째, 프로파일링을 포함하여 직접광고(direct marketing)를 목적으로 한 개인정보 처리에 반대하는 것은 어떠한 예외 없이 허용되며,[45] 이러한 경우 해당 개인정보는 더 이상 처리되어서는 안

42) GDPR Recital (68). "... 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..."

43) Kirsten Fiedler, Data protection series - issue sheets 06 - Data portability, European Digital Rights (2013.10.10.), *available at* https://edri.org/files/06-portability.pdf.

44) GDPR Art. 21. 1.

된다.[46] 셋째, 과학·역사 연구 또는 통계목적으로 개인정보가 처리되는 경우, 이러한 처리는 공익적 목적이 아닌 경우에 한하여 정보주체는 반대권을 행사할 수 있다. 다시 말하여, 공익에 기초한 과학·역사 연구 또는 통계 목적에 따른 개인정보의 처리에는, 해당 처리가 GDPR 제89조에 따른 안전조치를 구비하는 한, 반대권의 행사가 제한된다.

GDPR과 달리, 개인정보보호법에는 관련 규정이 존재하지 않는다. 개인정보보호법 제22조 3항은 직접 마케팅을 위하여 개인정보가 처리되는 경우, 정보주체가 이를 명확히 인지할 수 있도록 알리고 동의를 받도록 요구하고 있으나, 해당 조항만으로는 개인정보보호법이 GDPR의 반대권과 유사한 수준으로 정보주체의 권리를 보장하고 있다고 보기에는 무리가 따른다.

### 2.8. 정보주체 권리의 제한 (restrictions)

GDPR상 정보주체의 권리는 제3장 마지막 조항인 제23조에 따라 제한이 가능하다. 즉, GDPR은 상기 언급된 제3장에 따른 모든 정보주체의 권리에 일반적으로 적용되는 예외조항을 별도로 두고 있는 것이다. 동 조항은 정보주체의 권리에 제한을 가할 수 있는 구체적인 요건 및 절차를 구체적으로 규정하고 있다. 이에 따라 GDPR 제12조 내지 제22조에서 규정된 정보주체의 권리는 ① 국가안보, ② 국방, ③ 공공안전, ④ 범죄 예방·수사·적발·기소 또는 형 집행, ⑤ 기타 중요한 공익(특히 유럽연합 또는 회원국의 중요한 경제 및 재정적 이익), ⑥ 사법 독립성 및 사법 절차의 보호, ⑦ 법령에 따른 직업상 윤리 위반에 대한 예방, 수사, 적발 및 기소, ⑧ 경우에 따라서는 위 '⑥'을 제외한 나머지 경우에 있어서의 공적권한 행사에 대한 감시, 조사, 규제, ⑨ 정보주체 또는 제3자의 권리와 자유 보호, ⑩ 민사청구 집에 근거하여 제한될 수 있다.[47]

이러한 정보주체 권리의 제한은 상기 10가지 사항에 해당하는 경우 무조건적으로 허용되는 것이 아니라, 필요성과 비례성 원칙에 따른 법익형량에 근거하여 유럽연합 또는 회원국의 입법조치를 통하여 제한적으로 허용된다. 또한 이러한 입법조치는 최소한 다음 8가지 사항에 대하여 구체적인 조항을

45) GDPR Art. 21. 2.
46) GDPR Art. 21. 3.
47) GDPR Art. 23. 1.

마련하여야 한다. (① 처리 목적 또는 유형, ② 개인정보의 범주, ③ (도입된) 제한의 범위, ④ 남용이나 불법 접근 또는 전송 예방을 위한 보호수단, ⑤ 개인정보처리자의 구체적인 내역, ⑥ 저장기간, 처리(또는 처리 범주)의 성격·범위·목적을 고려한 적용 가능한 안전조치, ⑦ 정보주체의 권리와 자유에 대한 위험, ⑧ 제한의 목적을 해치지 않는 한, 정보주체가 제한에 대한 정보를 고지 받을 권리)[48]

개인정보보호법은 일반적인 예외조항으로서 제58조를 규정하고 있다. 이에 따라 정보주체의 권리를 다루고 있는 제5장을 포함하여 동 법 제3장 내지 제7장은 ① 공공기관이 처리하는 개인정보 중 「통계법」에 따라 수집되는 개인정보, ② 국가안전보장과 관련된 정보 분석을 목적으로 수집 또는 제공 요청되는 개인정보, ③ 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우로서 일시적으로 처리되는 개인정보, ④ 언론, 종교단체, 정당이 각각 취재·보도, 선교, 선거 입후보자 추천 등 고유 목적을 달성하기 위하여 수집·이용하는 개인정보에는 적용되지 않는다.[49] 그러나 이러한 제외 사유는 그 내용이 구체적이지 않고, 최소한의 안전장치와 같은 규정을 마련하고 있지 않다는 점에서 GDPR과 비교된다 하겠다.

## 2.9. 손해배상

개인정보보호법은 이외에도 정보주체의 권리를 규정하는 제5장에서 정보주체로 하여금 개인정보처리자의 동 법 위반에 따른 행위에 대하여 손해배상을 청구할 수 있음을 규정하고 있다.[50] GDPR에서 손해배상은 정보주체의 권리를 규정하고 있는 제3장이 아닌 제8장에서 별도로 규율되고 있다. 이에 따라 GDPR 제82조는 동 규정의 위반에 따라 물질적 또는 정신적 손해를 입은 여하한 자(any person)로 하여금 손해배상을 청구할 수 있도록 명시하고 있는데, 이는 정보주체 이외의 자에게도 손해배상 청구를 가능케 하였다는 점에서 개인정보보호법보다 보다 넓은 손해배상의 범위를 인정한 것이라 하겠다.[51]

48) GDPR Art. 23. 2.
49) 개인정보보호법 제58조 1항.
50) 개인정보보호법 제37조.
51) GDPR Art. 82.

## 3. Data Protection Impact Assessment

GDPR에서 규정하는 “Data Protection Impact Assessment(이하 DPIA)”는 개인정보보호법에서 규율하는 ‘개인정보보호 영향평가(이하 영향평가)’와 그 용어의 의미가 거의 동일하다. 그러나 두 제도는 용어의 의미만 유사할 뿐, 평가의 주체·평가방식·평가시점 등에서 차이를 보인다.

우선 GDPR 제35조에 규정된 DPIA의 주체는 개인정보처리자이다. DPIA 평가의 대상은 정보주체의 권리와 자유에 대한 심각한 위험(high risk)을 야기할 가능성이 높은 여하한 개인정보처리의 유형으로서, 그러한 개인정보처리 유형을 판단함에 있어서 GDPR 제35조 3항은 구체적인 기준과 사례를 제시하고 있다. 이에 따라 ① 프로파일링 등 개인적 측면에 대한 체계적이고 광범위한 자동화 처리, ② GDPR 제9조 1항에 규정된 특정 범주의 개인정보에 대한 대규모 처리 또는 제10조에 규정된 범죄경력 및 범죄 행위에 관련된 개인정보에 대한 처리, ③ 공개적으로 접근 가능한 지역에 대한 대규모의 체계적 모니터링을 하는 경우 개인정보처리자는 반드시 DPIA를 시행하여야만 한다.[52] 또한 감독당국(supervisory authority)은 DPIA가 요구되는 개인정보 처리의 목록을 작성하여 대중에게 공개하여야만 하고,[53] 동 평가가 요구되지 않는 개인정보 처리의 목록 역시 재량으로 공개할 수 있다.[54]

DPIA는 개인정보처리가 해당 개인정보를 처리하기 ‘이전에’ 처리에 따른 위험성을 사전에 예측하기 위하여 실시된다.[55] 이러한 자체적인 평가 결과, 정보주체의 권리와 자유를 침해할 심각한 위험이 존재한다고 판단되는 경우, 개인정보처리자는 해당 정보를 처리하기 이전에 감독당국과 반드시 사전협의(prior consultation)를 거쳐야만 한다.[56] 사전협의를 내용과 절차를 세부적으로 규정하고 있는 GDPR 제36조에 따라, 감독당국은 관리자와 상의하는 과정에서 해당 개인정보의 처리가 GDPR을 위반할 가능성이 있다고 판단되는 경우, 의견개진, 개선권고, 처리의 금지 등을 모두 포함하는 일련의 권한

52) GDPR Art. 35. 3.
53) GDPR Art. 35. 4.
54) GDPR Art. 35. 5.
55) GDPR Art. 35. 1.
56) GDPR Art. 36. 1.

을 행사할 수 있다.[57]

이와 달리, 개인정보보호법 제33조에서 규정하는 영향평가는 공공기관의 장이 평가기관에 의뢰하여 시행한다.[58] GDPR과 달리 개인정보처리자가 실시하는 영향평가는 동조 8항에 따라 권고사항에 불과하다. 영향평가의 대상이 되는 개인정보파일은 대통령령 제35조에 제시하는 기준에 따라 5만명, 50만명, 100만명 등 산술적 기준에 근거하여 산출된다.[59] 영향평가의 결과는 행정자치부장관에게 제출되며, 행정자치부장관은 보호위원회의 심의·의결을 거쳐 평가 결과에 대한 의견을 개진할 수 있다.[60]

이상을 토대로 개인정보보호법에 따른 영향평가와 GDPR에 따른 DPIA를 비교하면 다음과 같다. 첫째, 평가 주체 및 평가 시점과 관련하여, 개인정보보호법은 이미 운용되고 있는 대규모 개인정보파일의 처리에 대한 위험성을 제3자인 평가기관으로 하여금 평가하도록 규정하고 있는 반면, GDPR은 개인정보 처리 이전에 개인정보처리자로 하여금 이에 대한 위험성을 스스로 평가하도록 요구하고 있다. 둘째, 평가 대상이 되는 개인정보의 유형과 관련하여, 산술적 기준에 근거하여 영향평가의 대상을 선정하는 개인정보보호법과 달리, GDPR은 '정보주체의 권리와 자유에 심각한 위험을 수반하는 개인정보 처리'를 평가 대상으로 삼고 있다는 점에서 후자의 접근방식이 조금 더 유연하다고 볼 수 있다. 마지막으로 셋째, 평가 결과에 대한 사후 조치 및 감독기관의 권한과 관련하여, 개인정보보호법은 행정자치부장관으로 하여금 의견을 개진할 수 있음을 규정하고 있는 반면, GDPR은 사전협의 절차를 통하여 GDPR 위반 가능성이 높은 개인정보 처리에 대하여 처리의 금지를 포함한 구속력 있는 제재를 감독당국이 내릴 수 있도록 규정하고 있다는 차이가 존재한다.

---

57) GDPR Art. 36. 2.

58) 개인정보보호법 제33조 1항.

59) 개인정보보호법 시행령 제35조(개인정보 영향평가의 대상) 법 제33조제1항에서 "대통령령으로 정하는 기준에 해당하는 개인정보파일"이란 개인정보를 전자적으로 처리할 수 있는 개인정보파일로서 다음 각 호의 어느 하나에 해당하는 개인정보파일을 말한다. 1. 구축·운용 또는 변경하려는 개인정보파일로서 5만명 이상의 정보주체에 관한 법 제23조에 따른 민감정보(이하 "민감정보"라 한다) 또는 고유식별정보의 처리가 수반되는 개인정보파일 2. 구축·운용하고 있는 개인정보파일을 해당 공공기관 내부 또는 외부에서 구축·운용하고 있는 다른 개인정보파일과 연계하려는 경우로서 연계 결과 50만명 이상의 정보주체에 관한 개인정보가 포함되는 개인정보파일 3. 구축·운용 또는 변경하려는 개인정보파일로서 100만명 이상의 정보주체에 관한 개인정보파일.

60) 개인정보보호법 제33조 3항.

## 4. 행동강령 (Codes of Conduct)

GDPR 제40조에 따라 개인정보처리자 또는 수탁처리자를 대표하는 단체 또는 기관은 자체적인 행동강령을 마련할 수 있다.[61] 행동강령은 동종의 기업들이 가지고 있는 특별한 사정을 반영하여, 이들로 하여금 GDPR상의 의무를 준수할 수 있도록 도와주는 일종의 가이드라인 역할을 한다. 사회 여러 분야에서 처리되는 각기 다른 개인정보의 유형을 GDPR을 통하여 일일이 세부적으로 규율하기에는 현실적으로 많은 어려움이 따른다. 이처럼 GDPR이 특정 업종에서 다루는 특정 유형의 개인정보 처리에 대하여 구체적이고 세부적인 규정을 규율할 수 없는 상황에서, 행동강령은 GDPR의 원활한 적용과 준수를 위한 가이드라인 역할을 하는 것이다.

GDPR의 적용 및 준수를 확보하기 위하여 행동강령은 (a) 공정하고 투명한 처리, (b) 특정 상황에서 정보처리자가 추구하는 정당한 이익, (c) 개인정보의 수집, (d) 개인정보의 가명처리, (e) 일반 대중 및 정보주체에게 제공되는 정보, (f) 정보주체의 권리 행사, (g) 아동에게 제공되는 정보, 아동에 대한 보호와 부모의 책임을 지닌 자의 아동에 관련한 동의를 취득할 수 있는 방식, (h) 제24조 및 제25조에 규정된 조치와 절차와 제32조에 규정된 처리의 보안을 보장하기 위한 조치, (i) 감독기관 및 정보주체에게 개인정보 유출에 대해 통지, (j) 제3국이나 국제기구로 개인정보 이전, (k) 정보주체의 권리를 침해하지 않고, 개인정보처리자와 정보주체 간의 분쟁을 해결하기 위한 재판외 절차와 기타 분쟁 해결 절차에 관한 구체적인 규정을 마련할 수 있다.[62] 이처럼 행동강령은 특정 개인정보 처리가 실무에서 어떻게 규율될 수 있는지를 사례 중심적으로 다룰 수 있다는 점에서 개인정보처리자에게 현실적으로 많은 도움을 줄 수 있을 것으로 예상된다.

회원국, 감독당국, 유럽개인정보보호위원회, 유럽위원회는 이러한 행동강령의 제정을 장려해야 한다. 또한 행동강령의 준수 여부는 수탁처리자의 안전조치의무(제28조), 개인정보처리자의 안전조치의무(제32조)에 대한 준수 여부를 판단함에 있어서 하나의 판단기준이 되고 있다.

61) GDPR Art. 40. 1.
62) GDPR Art. 40. 2.

행동강령은 반드시 승인받아야 한다. 특정 업종을 대변하는 기관 또는 단체에 의하여 제정된 행동강령이 오직 하나의 회원국에만 영향을 미치는 경우, 해당 강령은 소관감독당국(해당 회원국의 감독당국)으로부터 승인받아야 하며,[63] 행동강령이 복수의 회원국에서 발생하는 개인정보 처리를 규정하고 있는 경우, 그러한 행동강령은 유럽개인정보보호위원회의 심의를 거쳐 유럽위원회의 최종 승인을 받아야 한다.[64]

행동강령의 이행을 확보하기 위하여 감시기관이 설립될 수 있다.[65] 이러한 감시기관은 소관감독당국의 인가를 받기 위하여 다음의 네 가지 요건을 충족시켜야만 한다. (① 독립성 및 전문성, ② 행동강령 준수 여부를 평가하기 위한 절차의 구비, ③ 개인정보 침해가 발생한 경우 침해에 대한 항의에 대처할 수 있는 능력, ④ 기관의 업무로 인하여 이해충돌이 발생하지 않을 것이란 사실에 대한 증명)[66] 다만, 행동강령의 제정 및 감시기관의 설립은 GDPR에 따른 의무사항은 아니다.

개인정보보호법은 GDPR과 달리 행동강령에 대한 규정을 두고 있지 않다. 다만, 행정자치부는 최근 GDPR의 행동강령과 목적과 취지가 유사한'개인정보보호 자율규제단체 지정 등에 관한 규정' 제정안을 행정예고 하고 의견수렴에 돌입한 바 있다.

## 5. 개인정보의 국외이전

GDPR은 제5장에서 개인정보의 국외이전을 방대하게 규율하고 있다. 이에 따라 개인정보가 이전될 것으로 예상되는 제3국 또는 국제기구의 개인정보보호 수준이 유럽연합의 수준보다 못 미치는 경우, 개인정보의 국외이전은 허용되지 않는다.[67] 특히 주목할 점은 GDPR에서 규율하고 있는 국외이전의 범위가 유럽연합에서 국외로 이전되는 최초의 이전뿐만 아니라 향후 발생할 수 있는 제3국(또는 국제기구)에서 또 다른 제3국(또는 국제기구)으로의 이전을 포함한다는 사실이다.[68]

63) GDPR Art. 40. 6.
64) GDPR Art. 40. 7.
65) GDPR Art. 41. 1.
66) GDPR Art. 41. 2.
67) GDPR Art. 44.
68) GDPR Art. 44.

GDPR에 따라 국외이전이 허용되는 경우는 다음과 같다. 첫째, 적합성 결정(adquacy decision)에 따른 이전이다. GDPR 제45조에 따라 유럽위원회는 특정 제3국 또는 국제기구의 개인정보보호 수준이 개인정보 이전을 허용할 만큼 적합한 수준인지를 결정할 수 있다. 이러한 적합성 결정은 동조 제2항에 따라 제3국 또는 국제기구의 인권수준, 독립된 소관감독기관의 존재 등 여러 평가기준에 근거하여 결정된다.[69] 이러한 평가기준에 근거하여 제3국 또는 국제기구가 개인정보의 적절한 보호수준을 구비하였다고 판단되는 경우, 개인정보의 국외이전은 허용될 수 있다. 적합성 결정은 정기적인 주기에 걸쳐 이루어지며, 이에 따라 기존에 허용되었던 개인정보의 국외이전에 대한 철회 역시 가능하다.[70]

둘째, 적절한 안전장치(approprate safeguards)에 따른 이전이다. GDPR 제45조에서 규율하고 있는 적절한 안전장치에는 다음의 경우가 포함된다. (① 공공기관 또는 단체 간 작성된 법적 문서 ② 구속력있는 기업규칙(binding corporate rules), ③ 제93조 2항에 따라 유럽위원회가 채택한 “표준개인정보보호조항(standard data protection clauses)”, ④ 제93조 2항에 따라 감독당국이 채택하고 유럽연합위원회가 승인한 표준개인정보보호조항, ⑤ 제40조에 따라 승인된 행동강령, ⑥ 제42조에 따라 승인된 인증메커니즘).[71] 이에 따라 적합성 결정이 이루어지지 않은 국가라 하더라도, ① 개인정보처리자 및 수탁처리자가 제시하는 적절한 안전장치가 존재하고, ② 정보주체의 권리가 이

69) GDPR Art. 45. 2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements: (a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred; (b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and (c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

70) GDPR Art. 45. 5.

71) GDPR Art. 46. 2.

행가능(enforceable)하며, ③ 정보주체를 위한 실효적인 법적 구제책이 마련되는 경우에 한하여, 해당 국가로의 정보이전은 제한적으로 허용된다 하겠다.[72]

개인정보보호법은 제14조 2항에서 “정부는 개인정보 국외 이전으로 인하여 정보주체의 권리가 침해되지 아니하도록 관련 시책을 마련하여야 한다.”라고 규정하고 있다.[73] 또한 동 법 제17조 3항은 국외의 제3자에 대한 개인정보 제공의 경우, ① 개인정보를 제공받는 자, ② 개인정보를 제공받는 자의 개인정보 이용 목적, ③ 제공하는 개인정보의 항목, ④ 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간, ⑤ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용을 정보주체에게 알리고 동의를 받을 것을 요구하고 있다.[74] 그러나 제14조 2항은 정부의 책무를 규정한 선언적·원칙적 규정이라는 점, 제17조 3항에서 규정하는 개인정보처리자의 고지의무는 동 조 제2항에 따른 국내 제3자에 대한 제공과 다르지 않다는 점을 살펴볼 때, 개인정보보호법이 국외이전과 관련된 세부적이고 상세한 제도와 절차를 구비하고 있다고 보기에는 무리가 있다.

## 6. 독립감독기구

유럽연합의 각 회원국은 GDPR의 이행을 감시하기 위하여, 하나 또는 그 이상의 독립된 감독당국(supervisory authority)을 설치해야 한다.[75] 감독당국은 독립성이 보장된 국가기관으로서 그 임무(제57조)와 권한(제58조)은 다음과 같다.

[표 2-1] 감독당국의 임무[76]

| |
|---|
| (a) 본 규정의 적용에 대한 모니터링 및 집행; |
| (b) 처리와 관련된 위험, 규칙, 안전조치 및 권리에 대한 대중의 인식제고와 이해촉진. 구체적으로 어린이를 다루는 활동의 경우, 각별한 주의가 요구됨; |
| (c) 회원국 법률, 국가 의회, 정부 및 다른 기관 및 기구에 따라, 처리와 관련한 개인의 권리 및 자유의 보호에 대한 법률 및 행정 조치에 대한 자문; |
| (d) 본 규정 의거한 정보처리자 및 수탁처리자의 각자 의무에 대한 인식 제고; |

72) GDPR Art. 46. 1.
73) 개인정보보호법 제14조 2항.
74) 개인정보보호법 제17조 3항.
75) GDPR 제54조는 감독당국의 설립에 관한 절차를 자세히 규정하고 있다.
76) GDPR Art. 57. 1.

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

(f) 정보주체나 기구, 기관 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, 그러하다;

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

(h) 기타 감독기관이나 공공기관으로부터 수령 받은 정보 등을 근거로 본 규정의 적용에 대한 조사 실시;

(i) 특히 정보통신기술 및 상업적 관행의 개발 과정에서 개인정보 보호에 영향을 미치는 범위에서 관련전개(developments) 상황에 대한 모니터;

(j) 제28조의 (8)항과 제46조 (2)항의 (d)에 규정된 정보보호 표준계약조항(standard contractual clauses)의 채택;

(k) 제35조의 (4)항에 따라 개인정보보호 영향평가에 대한 요건과 관련한 목록을 수립 및 유지;

(l) 제36조 (2)항에 규정된 처리 작업에 관한 자문 제공;

(m) 제40조에 의거한 행동강령의 마련을 장려하고 의견을 제시하며, 제40조 (5)항에 따라 충분한 안전조치를 제공하는 행동강령을 승인;

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

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

(p) 제41조에 의거한 행동강령의 모니터링 기구 및 제43조에 의거한 인증 기구의 인가에 대한 기준의 초안 마련 및 공표;

(q) 제41조에 의거한 행동강령의 모니터링 기구의 및 제43조에 의거한 인증기관의 인가 시행;

(r) 제46조 (3)항에 규정된 계약조항 및 조문에 대한 승인;

(s) 제47조에 의거한 의무적 기업규칙(biding corporate rules)에 대한 승인;

(t) 유럽정보보호이사회의 활동에 기여;

(u) 본 규정의 위반과 제58조 (2)항에 따라 취해지는 조치에 대한 내부적 기록 보관;

(v) 개인정보 보호와 관련된 기타 업무 수행;

[표 2-2] 감독당국의 권한[77]

**- 감독당국의 조사권한 (investigative powers) -**

(a) 정보처리자와 수탁처리자 그리고 해당되는 경우, 정보처리자 또는 수탁처리자의 대리인에게 업무의 수행에 필요한 정보의 일체를 제공하도록 명령;

(b) 개인정보보호 감사의 형식의 조사 실시;

(c) 제42조 (7)항에 의거하여 발급된(issued) 인증에 대한 검토 실시;

(d) 정보처리자 또는 수탁처리자에게 본 규정의 위반 혐의 사안의 통지;

(e) 정보처리자 또는 수탁처리자로부터 업무의 수행에 필요한 모든 개인정보 및 모든 정보에 대한 열람권 취득;

(f) 유럽연합 또는 회원국의 절차 법률에 따라, 모든 개인정보 처리 장치 및 수단 등, 정보처리자와 수탁처리자의 영역에 대한 열람권 취득;

**- 감독당국의 시정 권한 (corrective powers) -**

(a) 예정된 처리작업(들)이 본 규정의 조문을 위반할 가능성이 높은 것에 대해 정보처리자 또는 수탁처리자에게 경고 발령;

(b) 예정된 처리작업(들)이 본 규정의 조문을 위반한 경우, 정보처리자 및 수탁처리자를 견책;

(c) 정보처리자 및 수탁처리자가 본 규정에 따라 본인의 권리를 행사하고자 하는 정보주체의 요청을 따를 것을 지시;

(d) 정보처리자 또는 수탁처리자에게 처리작업(들)이 본 규정의 조문을 준수하도록 지시하며, 적절한 경우, 구체적인 방식과 구체적인 기간 내에 하도록 지시;

(e) 정보주체에게 개인정보 유출에 대해 통지하도록 정보처리자에게 지시;

(f) 처리에 대한 금지 등, 임시 또는 확정적 제한의 부과;

(g) 제16조, 제17조, 제18조에 따른 처리의 수정이나 삭제 또는 제한을 지시하고, 제17조 (2)항 및 제19조에 따라 개인정보를 제공 받는 수령인들에게 이러한 행동조치에 대한 통지를 지시;

(h) 인증의 요건이 충족되지 않거나 더 이상 충족되지 않는 경우, 인증을 철회하거나 인증기구에게 제42조 및 제42조에 의거하여 발급된 인증을 철회하라고 지시하거나 인증기구에게 인증을 발급하지 않도록 지시;

(i) 각 개별 상황 별 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.

77) GDPR Art. 58.

- 감독당국의 인가 및 자문 권한 (authorisation and advisory powers) -

(a) 제36조에 규정된 사전 자문의 절차에 따라 정보처리자에게 자문을 제공;

(b) 자체 재량이나 요구에 따라, 해당 국가의 국회, 회원국의 정부 또는 회원국 법률에 따라 다른 기관 및 기구와 대중에게 개인정보보호와 관련한 사안에 대한 의견을 제공;

(c) 회원국 법률에서 사전 승인을 요구하는 경우, 제36조 (5)항에 규정된 처리에 대한 승인;

(d) 제40조 (5)항에 따른 의견 제공 또는 행동강령의 초안에 대한 승인;

(e) 제42조에 따른 인증기구의 인가;

(f) 제42조 (5)항에 따른 인증 발급 또는 인증의 기준에 대한 승인;

(g) 제28조 (8)항 및 제46조 (2)항에 규정된 정보보호 표준조항의 채택;

(h) 제46조 (3)항의 (a)에 규정된 정보보호 계약조항에 대한 승인;

(i) 제46조의 (3)항의 (b)에 규정된 행정적 협약에 대한 승인;

(j) 제47조에 따른 의무적 기업규칙에 대한 승인.

또한 GDPR은 복수의 감독당국으로 인한 업무의 혼란과 중복을 방지하기 위하여, 감독기관 사이의 협력과 일관성(cooperation and consistency)을 강조하고 있다. 예를 들어 GDPR 제56조는 개인정보처리자 및 수탁처리자의 주된 사업지(main establishment)가 존재하는 국가의 감독당국을 '주된 감독당국(lead supervisory authority)'으로서 규정하고 있다. GDPR 제4조 (16)에 따라 주된 사업지는 반드시 하나의 사업지로 지정되어야하므로, 복수의 회원국에서 처리되는 개인정보를 소관하는 주된 감독당국 역시 단일화 될 수 있는 것이다. 이에 따라 한 기업이 유럽연합내 복수 회원국에서 활동한다 하더라도, 해당 기업에 대한 관리·감독의무, 개인정보보호 업무의 책임소재 등을 하나의 감독당국에게 귀속시킬 수 있게 된다.

개인정보보호법에서 규정하는 소관기관으로는 행정자치부와 개인정보보호위원회가 존재한다. 먼저 행정자치부는 개인정보보호법상 개인정보 관리 실태 등에 대한 자료 제출을 요구할 수 있으며(제11조), 개인정보보호지침을 정할 수 있고(제12조), 개인정보보호와 관련된 시책을 마련하는(제13조) 등의 업무를 담당한다. 또한 행정자치부는 주민등록번호의 분실·도난·유출·위조·변조에

따른 과징금 부과(제34조의2) 등의 권한을 가지고 있다. 다음으로, 대통령 직속기관인 개인정보보호위원회는 동 법 제8조에 따라 개인정보와 관련된 여러 사항을 심의·의결하고, 이러한 사항을 심의·의결하기 위하여 관련 조치를 취할 수 있다.[78] 특히 최근 신설된 개인정보보호법 제8조 3항 내지 5항에서 나타나는 바와 같이, 개인정보보호위원회는 개정을 통하여 그 권한이 점차 강화되고 있는 추세이다.[79]

## 7. 유럽개인정보보호위원회

GDPR의 신설로 인하여 1995년 개인정보보호지침에 따른 제29조 작업반(Article 29 Working Party)는 폐지되고, 유럽개인정보보호위원회가 이를 대체하게 된다. 각 회원국 감독당국의 장으로 이루어진다는 점에서 유럽개인정보보호위원회의 인적구성은 제29조 작업반과 거의 동일하다. 다만, 유럽개인정보보호위원회는 제29조 작업반과 같이 단순한 심의기구가 아니라, 독립된 법인격을 가지고 의장(Chair)의 지휘 하에 운영되는 독립된 기구라는 차이가 있다. 예를 들어, 제29조 작업반의 사무장(Secretary)은 유럽위원회 소속 공무원이었으나, 유럽개인정보보호위원회의 사무장은 위원회의 구속을 받지 않는 독립적인 지위를 가진다.[80]

유럽개인정보보호위원회의 가장 중요한 역할은 GDPR의 일관된 적용을 위하여 가이드라인, 권고, 의견 등을 개진하고 관련 모범사례를 발행하는 것이

---

78) 개인정보보호법 제8조(보호위원회의 기능 등) ① 보호위원회는 다음 각 호의 사항을 심의·의결한다. 1. 제9조에 따른 기본계획 및 제10조에 따른 시행계획 2. 개인정보 보호와 관련된 정책, 제도 및 법령의 개선에 관한 사항 3. 개인정보의 처리에 관한 공공기관 간의 의견조정에 관한 사항 4. 개인정보 보호에 관한 법령의 해석·운용에 관한 사항 5. 제18조제2항제5호에 따른 개인정보의 이용·제공에 관한 사항 6. 제33조제3항에 따른 영향평가 결과에 관한 사항 7. 제61조제1항에 따른 의견제시에 관한 사항 8. 제64조제4항에 따른 조치의 권고에 관한 사항 9. 제66조에 따른 처리 결과의 공표에 관한 사항 10. 제67조제1항에 따른 연차보고서의 작성·제출에 관한 사항 11. 개인정보 보호와 관련하여 대통령, 보호위원회의 위원장 또는 위원 2명 이상이 회의에 부치는 사항 12. 그 밖에 이 법 또는 다른 법령에 따라 보호위원회가 심의·의결하는 사항 ② 보호위원회는 제1항 각 호의 사항을 심의·의결하기 위하여 필요한 경우 다음 각 호의 조치를 할 수 있다. 1. 관계 공무원, 개인정보 보호에 관한 전문 지식이 있는 사람이나 시민사회단체 및 관련 사업자로부터의 의견 청취 2. 관계 기관 등에 대한 자료제출이나 사실조회 요구

79) 개인정보보호법 제8조(보호위원회의 기능 등) ③ 제2항제2호에 따른 요구를 받은 관계 기관 등은 특별한 사정이 없으면 이에 응하여야 한다. ④ 보호위원회는 제1항제2호의 사항을 심의·의결한 경우에는 관계 기관에 그 개선을 권고할 수 있다. ⑤ 보호위원회는 제4항에 따른 권고 내용의 이행 여부를 점검할 수 있다.

80) GDPR Art. 75. 2.

다.[81] 예를 들어, 유럽개인정보보호위원회는 적합성 평가를 시행하는 과정에서 제3국의 개인정보보호 수준을 판단함에 있어서 유럽위원회에 의견을 제시할 수 있으며, GDPR의 해석에 대한 권고적 의견도 제시할 수 있고, 개인정보보호와 관련된 정기보고서를 매년 제출해야한다. 이러한 역할은 1995년 개인정보보호 지침에 따른 제29조 작업반의 업무와 유사하다 할 수 있다.

독립성이 보다 강화되었다는 점 이외에도, 유럽개인정보보호위원회는 제29조 작업반과 다음과 같은 차이를 가진다. 첫째, 특정 사안에 대하여 제29조 작업반이 제시하는 의견(opinion)이 감독당국의 결정 이후에 이루어질 수 있

81) GDPR Art. 70. 유럽개인정보보호위원회는 다음의 업무를 수행한다. (a) 제64조 및 제65조에 규정된 경우에서 본 규정의 올바른 적용 여부를 모니터링하고 보장; (b) 본 규정의 개정안을 포함하여 유럽연합 역내의 개인정보 보호와 관련된 문제에 대해 집행위원회에 자문을 제공; (c) 구속력있는 기업규칙에 관해 정보처리자, 수탁처리자, 감독기관 간에 이루어지는 정보 교환의 양식 및 절차에 대해 집행위원회에 자문을 제공; (d) 제17조(2)에 명시된 대로 일반에 공개되는 통신 서비스로부터 개인정보의 링크, 사본 또는 복제본을 삭제하기 위한 절차에 대해 가이드라인, 권고사항 및 모범사례를 발행; (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 발행; (f) 제22조(2)에 따른 프로파일링을 기반으로 하는 결정의 기준 및 조건을 추가로 명시하기 위해 본 호의 (e)에 부합하는 가이드라인, 권고사항 및 모범사례를 발행; (g) 개인정보 침해를 규명하고 제33조(1) 및 (2)에 명시된 부당한 지체를 결정하기 위해서, 그리고 정보처리자 또는 수탁처리자가 개인정보 침해에 대해 고지해야 하는 특정 상황에 대하여 본 호의 (e)에 부합하는 가이드라인, 권고사항 및 모범사례를 발행; (h) 개인정보 침해가 제34조(1)에 명시된 개인의 권리와 자유에 대한 중대한 위험을 초래할 가능성이 있는 상황에 대해 본 호의 (e)에 부합하는 가이드라인, 권고사항 및 모범사례를 발행; (i) 정보처리자가 준수하는 의무적 기업 규칙과 수탁처리자가 준수하는 의무적 기업 규칙 및 제47조에 명시된 관련 정보주체의 개인정보 보호를 보장하기 위한 추가적 필요요건을 기반으로 개인정보 이전의 기준 및 요건을 추가로 명시하기 위해 본 호의 (e)에 부합하는 가이드라인, 권고사항 및 모범사례를 발행; (j) 제49조(1)를 근거로 하는 개인정보 이전에 대한 기준 및 요건을 추가로 명시하기 위해 본 호의 (e)에 부합하는 가이드라인, 권고사항 및 모범사례를 발행; (k) 감독기관을 위해 제58조(1), (2) 및 (3)에 명시된 조치의 적용 및 제83조에 따른 행정 과태료 책정에 관한 가이드라인을 수립; (l) (e) 및 (f)에 명시된 가이드라인, 권고사항 및 모범사례의 실제 적용을 검토; (m) 제54조(2)에 따라 개인이 본 규정의 침해를 신고하기 위한 보편적 절차 수립에 대해 본 호의 (e)에 부합하는 가이드라인, 권고사항 및 모범사례를 발행; (n) 제40조 및 제42조에 따른 행동강령의 수립 및 개인정보보호 인증 메커니즘, 보호 인장과 마크의 구축을 장려; (o) 제43조에 따라 인증 기구의 인가 및 정기 검토를 실시하고 제43조(6)에 따라 인가된 기구 및 제42조(7)에 따라 제3국에 설립된 공인 정보처리자 또는 수탁처리자의 공공기록부(public register)를 유지; (p) 제42조에 따라 인증 기구의 인가를 목적으로 제43조(3)에 명시된 요건을 지정; (q) 제43조(8)에 명시된 인증 요건에 관한 의견서를 집행위원회에 제공; (r) 제12조(7)에 명시된 아이콘에 관한 의견서를 집행위원회에 제공; (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 제공; (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 발행; (u) 감독기관들 사이에서의 협력 및 효과적인 양자간·다자간 정보와 모범사례 교류를 촉진; (v) 공통의 교육 프로그램을 장려하고 감독기관들 간에, 그리고 적절한 경우 제3국의 감독기관들이나 국제기구와의 인적 교류를 시행; (w) 전 세계 개인정보보호 감독기관들과의 정보보호 법률 및 관행에 대한 지식과 자료의 교류를 촉진; (x) 제40조(9)에 따라 유럽연합 차원에서 수립된 행동강령에 관한 의견서를 발부; (y) 일관성 메커니즘에서 처리되는 사안에 대하여 감독기관 및 법원이 채택한 결정의 공개 전자 기록부(electronic register)를 유지.

다는 비판이 제기된 바, GDPR 체제에서는 유럽개인정보보호위원회의 의견이 채택되지 않은 시점에서, 감독당국의 결정이 이루어질 수 없다. 둘째, 제29조 작업반과 달리, 유럽개인정보보호위원회는 각 감독당국 사이에 존재하는 분쟁을 조정하는 역할을 하게 되었으며, 이 경우 유럽개인정보보호위원회가 내리는 결정은 구속력이 있다. 개인정보보호법에는 유럽개인정보보호위원회와 비슷한 역할을 담당하는 기구가 존재하지 않는다.

## 8. 현행 개인정보보호법 개정방안

이상에서 논의된 점을 종합적으로 검토할 때, GDPR의 입법례는 현행 개인정보보호법 개정에 있어서 다음과 같은 가이드라인 역할을 제공할 수 있을 것이다. 첫째, 개인정보보호법은 개인정보보호의 또 다른 원칙으로서 투명성 원칙을 규정하여, 개인정보처리자로 하여금 쉽고 분명한 언어의 사용을 통한 정보주체의 적절한 권리행사를 보장할 수 있다.[82] 둘째, 개인정보보호법은 SNS와 같은 인터넷서비스 이용 과정에서 아동에 대한 보호의 필요성을 특별히 강조하고, 이와 관련된 규정을 마련하고 있는 GDPR의 입법을 참고할 필요가 있다.[83] 셋째, 개인정보보호법은 개인정보보호 강화를 위하여 GDPR에서 규율하고 있는 개인정보주체의 권리를 새롭게 반영하거나, 기존의 권리를 보다 상세하게 규율할 필요가 있다. 개인정보보호법이 규율하지 않고 있는 GDPR의 규정으로는 잊혀질 권리, 자기정보 이전에 관한 권리, 프로파일링을 비롯한 개인에 관한 자동의사결정(Automated individual decision making)에 종속되지 않을 권리 등이 존재한다. 자기정보 이전에 관한 권리는 빅데이터 시대에 정보주체의 자기정보에 대한 결정권을 강화하는 한편 스타트업기업과 소규모업체에게는 디지털시장에서 대기업에게 선점된 개인정보시장(data market)에 접근할 수 있는 기회를 제공함으로써 기업 간 경쟁과 혁신을 증진시킬 것으로 기대할 수 있다. 개인정보보호법에서 규율하고 있는 열람권, 삭제권 및 정정권 역시 GDPR의 유사 규정을 참고하여 보다 상세하게 규율될 필요가 있다. 넷째, 개인정보보호법은 동법 제37조에 따른 영향평가 이외에, GDPR의 Data Protection Impact Assessment와 같은 유형의 사전평가제를 도입할 수 있다. 전술한 바와 같이, 개인정보보호법상의 영향평가는 이미 운용되고 있는 대규모 개인정보파일의 처리에 대한 위험성을

82) GDPR, Art. 12.
83) GDPR Art. 8, Art. 17 1.

제3자인 평가기관으로 하여금 평가하도록 하는 반면, GDPR에서는 개인정보처리가 이루어지기 이전에 개인정보처리자로 하여금 이에 대한 위험성을 자체적으로 평가하는 것으로 양자는 구별된다. GDPR은 사전평가의 결과, 해당 개인정보의 처리가 위험하다고 판단되는 경우, 사전협의 과정에서 감독당국으로 하여금 처리의 금지를 포함하여 구속력 있는 제재를 가할 수 있도록 규정하고 있는 바,[84] 개인정보보호법에서 이처럼 개인정보침해의 위험성을 사전에 평가하고 개인정보침해 위험을 사전에 저감할 수 있는 관련 규정을 마련한다면. 효과적인 안전장치로 기능할 수 있을 것이다. 다섯째, 행동강령에 대한 GDPR의 규정을 참고하여, 개인정보보호법은 개인정보보호에 관한 실무에 있어서 동종 사업에 임하는 개인정보처리자의 개인정보처리 방침에 관한 행동강령의 자체적인 제정을 법률로서 권고할 수 있다. 여섯째, 개인정보의 국외이전을 규율하고 있는 개인정보보호법 제14조 2항 및 제17조 3항은 그 실체적·절차적 규정이 상세하지 못하여 선언적 조항에 그치는 문제를 야기하는 바, 해당 조항들은 개인정보의 국외이전에 대하여 구체적이고 세부적인 규정을 마련하고 있는 GDPR의 관련 규정을 참조하여 개정될 필요가 있다.[85] 마지막으로 일곱째, GDPR이 개인정보보호에 있어서 감독당국의 독립성을 강조한다는 사실과, 이처럼 독립된 감독당국에게 방대한 임무와 막강한 권한을 부여하고 있다는 사실을 감안할 때, 대통령 직속기관으로서 개인정보보호위원회의 임무와 권한은 지금보다 더욱 강화될 필요가 있다. 특히 GDPR은 1995년 개인정보보호지침보다 법 적용대상이 확대됨에 따라 우리나라 기업에 직접 영향을 미칠 것으로 예상된다. 이러한 환경에 적극적으로 대응하기 위해서는 EU 역내 국가의 기업과 동등한 지위에서 활동할 수 있도록 'EU의 개인정보보호 적정성 평가' 통과가 필요하다. EU 적합성 평가 과정에서 위원회의 독립성과 임무와 권한이 쟁점이 될 수 있는 점에서 개인정보보호위원회의 임무와 권한의 확대는 매우 중요하다.

# III. 빅 데이터 분석 등 개인정보의 활용 방안

정보화 시대의 빅 데이터 분석, 오픈 데이터(open data) 등을 포함한 개인정보의 활용에 대한 사회·경제적 입법수요는 점차 증가하고 있는 추세이다. 그러나 빅 데이터 분석, 오픈 데이터 등을 포함한 21세기 자산으로서 정보의

84) GDPR Art. 35, Art. 36.
85) GDPR, Art. 44, Art. 45, Art. 46.

활용은 대개의 경우 개인정보의 처리를 수반하므로,[86] 개인정보보호와 개인정보를 활용한 시장가치의 창출은 이해가 대립되는 측면이 존재한다. 이러한 맥락에서 세계 주요 선진국들은 빅 데이터 분석을 포함한 대규모의 자동화된 방식에 의한 개인정보 처리에 있어서, 정보주체의 권리를 보호하는 한편, 정보의 활용을 통한 경제적 가치 창출을 도모하기 위한 균형 잡힌 입법방안을 모색하고 있다.

# 1. GDPR

## 1.1. 개인정보의 목적 외 처리

GDPR은 목적 외 처리에 대하여 상당히 유연한 접근을 취하고 있다. 제6조 4항에 따라 개인정보의 목적 외 처리가 허용되는 경우는 첫째, 목적 외 처리에 대한 정보주체의 동의를 얻는 경우, 둘째, 목적 외 처리가 - 제23조 1항에 명시된 일련의 목적을 보호하기 위하여 - 유럽연합 또는 회원국의 법률에 근거하는 경우,[87] 셋째, 개인정보가 최초로 수집될 때 제시된 목적과 다른 목적(another purpose)이 최초 수집 목적과 양립하는 경우이다.

> *Article 6 Lawfulness of processing*
>
> 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

86) 주목할 점은 모든 빅 데이터 분석이 개인정보보호법제의 적용을 받지 않는다는 사실이다. 이와 관련하여, 영국 정보보호위원회(Information Commissioner's Office, 이하 'ICO')는 개인정보를 이용하지 않은 빅 데이터 분석의 예를 들고 있다. 이러한 예에는 대중교통에 장착된 GPS를 기반으로, 지형 공간 데이터(geospatial data)를 이용한 교통정보의 예측, 기후·날씨 정보를 이용한 기상 예측 등이 존재한다. Information Commissioner's Office, Big Data and Data Protection, 28 July 2014, *available at* https://ico.org.uk/media/for-organisations/documents/1541/big-data-and-data-protection.pdf, paras. 34 - 39.

87) 제23조 1항에 규정된 목적으로는 국가안보, 방위, 공공안전, 범죄의 예방, 조사, 적발, 기소 또는 형사처분 집행(공공안전 확보 및 공공안전에 대한 위협의 예방을 포함), 그밖에 유럽연합 또는 회원국의 공익상 중요한 목적으로, 특히 유럽연합 또는 회원국의 중요한 경제적 또는 재정적 이익, 사법독립과 사법절차의 보호, 직업적 윤리의 위반에 대한 예방, 조사, 적발 및 기소, 상기 언급된 사항에 대한 공공기관의 감독 및 조사, 정보주체의 보호와 정보주체가 아닌 다른 사람의 권리와 자유, 민사청구의 집행이 존재한다.

collected and the purposes of the intended further processing;
(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;
(d) the possible consequences of the intended further processing for data subjects;
**(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.**

최초 수집 목적과 양립하는 다른 목적에 근거한 추가처리(further processing)를 허용하는 것은, 동 규정에 한정적으로 명시된 정보주체의 동의 또는 법률에 따른 예외사유 이외의 목적 외 처리를 폭 넓게 인정하는 것으로, 개인정보의 활용과 관련이 깊다. GDPR 제6조 4항은 이러한 양립가능성을 판단하기 위한 고려사항으로서 ① 최초 수집 목적과 추가처리를 위한 목적 사이의 연관성, ② 정보주체와 개인정보처리자의 관계를 고려하여, 해당 개인정보가 수집되는 전후 상황, ③ 제9조 내지 제10조에서 규정하고 있는 민감정보 및 범죄기록 처리 여부 등 처리되는 개인정보의 특성, ④ 의도된 추가처리가 정보주체에 미칠 수 있는 결과, ⑤ 적절한 안전조치(safeguards)[88]로서 암호처리(encryption) 또는 가명처리(pseudonymisation) 여부가 존재한다.[89] 만약 추

88) 동 보고서는 'safeguards'를 '안전조치'라는 용어로 서술하고 있으나, GDPR에서 서술되는 'safeguards'는 개인정보보호법 제29조 「안전조치의무」에서 규정하는 물리적·기술적·관리적 조치를 의미하는 안전조치와 구별되어야 한다. 개인정보보호법 제29조와 유사한 조항은 GDPR 제32조 「security of processing」으로서 동 조항에서 규정하는 'technical and organisational measure'가 국내법상 안전조치에 해당한다고 볼 수 있다. 이에 따라 제89조 등에서 명시하고 있는'safeguards'는 안전조치와 구분되기 위하여 '안전장치'로 서술될 수 있다. 동일한 맥락에서, GDPR 제32조는 '처리의 안보'가 아니라 '안전한 처리'로 풀이될 수 있다.

89) GDPR Art.6.4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia: (a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing; (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller; (c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10; (d) the possible consequences of the intended further processing for data subjects; (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

가처리를 위한 목적이 최초 수집 목적과 양립한다면, 이러한 목적 외 처리는 정보주체의 동의나 별도의 법적 근거 없이도 허용된다.[90]

이 가운데 빅 데이터 분석, 오픈 데이터 등 개인정보의 활용과 관련하여 주목할 규정은 제5조 1항(b)이다. 동 조항은 개인정보의 목적 외 처리를 원칙적으로 금지하면서도, 동 규정 제89조 1항에 따른 '공익을 위한 기록보존, 과학 및 역사 연구, 통계적 목적'은  수집 목적과 양립 가능한 것으로 간주된다고 규정하는 바, 이러한 목적에 따른 추가처리는 제89조 1항에서 규정하고 있는 안전조치(safeguards)를 구비하는 한, 목적 외 처리로서 허용되는 것이다.[91]

*Article 5 Principles relating to processing of personal data*

1. Personal data shall be:
(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)

이상을 요약하면, GDPR에서 빅 데이터 분석을 비롯한 개인정보의 활용은 다음의 근거에 의하여 목적 외 처리로서 허용될 수 있다. 첫째, 제6조 4항(e)에 따라 가명처리 또는 암호처리가 되어 있는 경우, 추가처리를 위한 목적이 최초 수집 목적과 양립 가능한 경우가 존재할 수 있다. 다만, 동 조항에 따른 안전조치는 양립 가능성을 판단하기 위한 하나의 고려사항에 불과하므로, 가명처리 또는 암호처리의 존재 자체가 목적 외 추가처리를 필연적으로 정당화시키는 것은 아니다. 둘째, 제5조 1항(b) 및 제89조 1항에 따라서, 공익을 위한 기록보존, 과학 및 역사 연구, 통계적 목적에 따른 개인정보 처리는,

90) GDPR Recital (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...).

91) 1. Personal data shall be: ... (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);

해당 처리가 가명처리를 포함한 안전조치를 구비하고 있는 한, 목적 외 처리로서 허용된다.

양자의 가장 큰 차이는 공익을 위한 기록보존, 과학 및 역사 연구, 통계적 목적을 위한 개인정보 처리의 경우, 최초 수집 목적과의 양립 가능성을 별도로 판단할 필요가 없다는 데 있다. 또한 두 경우에 있어서, 가명처리 또는 암호처리를 포함한 안전조치(safeguards)는 그 법적 지위가 다르다 할 것인데, 제6조 4항(e)에 근거하는 경우 안전조치는 양립 가능성을 판단하기 위한 고려사항에 불과한 반면, 제5조 1항(b)에서 언급하는 동 규정 제89조 1항에 따른 안전조치는 목적 외 처리를 허용하기 위한 필수적인 요건에 해당한다.

### 1.2. 공익을 위한 기록보존, 과학 및 역사 연구, 통계 목적

#### 1.2.1. 범위

공익을 위한 기록보존과 관련하여, 공익적 가치를 지닌 기록물을 보유하고 있는 공공당국 또는 공공·민간 기관이 수행하는 기록물의 획득, 보존, 평가, 편찬, 기술, 교환, 홍보, 배포, 제공은 목적 외 추가처리로서 허용된다.[92]

GDPR은 본 규정의 취지를 고려하여 과학적 연구 목적의 개인정보 처리는 폭 넓게 해석되어야 한다고 규정하고 있다. 이에 따르면, 과학적 연구란 기술의 발전과 실현, 기초연구, 응용연구 및 민간투자연구, 공중보건 분야에서 시행된 공공보건연구 등을 포함한다.[93] 특히 GDPR은 과학적 목적에 따른 개인정보 처리에 있어서 유럽연합 기능에 관한 조약 제179조 1항이 고려되어야 함을 언급하고 있는데, 동 조항은 과학자, 과학적 지식 및 기술이 자유

92) GDPR Recital (158) (...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...)

93) GDPR Recital (159) (...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...)

롭게 이동하는 'European Research Area'의 실현을 목적으로 삼고 있다. 역사연구에는 계보학연구가 포함된다.[94] 다만, 공익을 위한 기록보존과 마찬가지로, 역사연구를 목적으로 한 개인정보 처리에 있어서 사자의 개인정보는 동 규정의 적용을 받지 않는다.

통계 목적에 따른 개인정보 처리에 대하여 GDPR은 통계 내용(statistical content), 접근의 통제(control of access), 통계 목적에 따른 개인정보 처리에 대한 세부사항과 정보주체의 권리와 자유를 보호하고 통계의 기밀성을 보장하기 위한 적절한 조치를 유럽연합 또는 회원국의 법률이 결정해야함을 명시하고 있다. 통계 목적에 따른 개인정보 처리는 통계 조사 및 통계 결과를 작성하기 위하여 필요한 개인정보의 수집 및 처리의 작업 일체를 의미한다. 이러한 통계 결과는 과학적 목적을 포함한 다른 목적을 위하여 추가적으로 이용될 수 있다.[95]

특히, 통계 목적은 1) 통계 목적에 따른 처리의 결과가 개인정보가 아니라 데이터 집합체(aggregate data)라는 사실과, 2) 이러한 통계 처리의 결과나 통계에 이용된 개인정보는 어떠한 개인에 관한 조치나 결정을 지지하는데 활용되지 않았다는 사실을 의미한다.[96] 통계 목적과 관련된 GDPR의 상기 해설은 개인정보의 활용과 관련하여 매우 중요한 의미를 가진다. 통계를 위하여 이용된 정보에 개인정보가 포함되는 경우, 그러한 통계 처리는 GDPR의 적용을 받는 것이 당연지만, 통계 목적에 따른 개인정보 처리가 목적 외 처리로서 허용될 수 있는 이유는 그러한 통계 처리의 결과물이 개인정보가 아닌 데이터 집합체(aggregate data)로서 간주되기 때문이다. 이러한 맥락에서 후술하게 될 가명처리 및 익명처리는 통계 목적에 따른 개인정보의 활용

94) GDPR Recital (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.)

95) GDPR Recital (162) (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...)

96) GDPR Recital (162) (...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.)

과 밀접한 연관성을 가진다. 2013년 제29조 작업반은 통계 목적에 따른 개인정보 처리는 교통사고에 따른 사망자 통계와 같이 공익적인 목적뿐만 아니라, 시장조사를 목적으로 하는 빅 데이터 분석과 같은 상업용 목적을 포함한다는 의견을 명시적으로 제시한 바 있다.[97]

### 1.2.2. 기록보존, 과학·역사 연구, 통계 목적에 따른 목적 외 처리의 실효성 확보

빅 데이터 분석 등 개인정보의 활용을 통한 시장가치의 창출을 도모함에 있어서 가장 중요한 부분은 그러한 개인정보 처리를 어떠한 근거에 따라서 허용할 것인가에 대한 문제이다. 앞서 살펴본 바와 같이, GDPR에서 규정하는 개인정보의 목적 외 처리 - 특히, 공익을 위한 기록보존, 과학 및 역사 연구, 통계 목적에 따른 개인정보 처리 - 규정은 개인정보의 활용을 허용하는 근거가 될 수 있다.

그러나 목적 외 처리를 허용하기 위한 법적 근거를 구비하는 것과 마찬가지로 중요한 점은, 개인정보의 활용을 실효적으로 도모하기 위한 일관된 법 체계를 마련하는 것이다. 이러한 맥락에서 GDPR은 공익을 위한 기록보존, 과학 및 역사 연구, 통계 목적에 따른 개인정보의 활용과 관련하여 다음과 같은 관련 규정을 마련하고 있다.

첫째, GDPR은 상기 목적에 따라 개인정보를 활용하는 개인정보처리자에 대하여 특정 의무를 경감시키고 있다. 동 규정 제14조는 개인정보처리자가 정보주체 이외의 출처로부터 개인정보를 수집하는 경우, 개인정보처리자로 하여금 정보주체에게 자신에 대한 정보(기관명, 세부연락처 등), 처리의 목적과 근거, 처리되는 개인정보의 유형, 수령인, 국외이전에 관한 정보 등을 고지하도록 규정하고 있다. 그러나 동 조 제5항(b)는 개인정보처리자에게 '과도한 노력(disproportionate effort)'이 요구되고, 정보주체에 대한 고지가 공익을 위한 기록보존, 과학 및 역사 연구, 통계 목적에 따른 개인정보 처리를 불가능하게 만들거나 그러한 목적의 달성을 심각하게 저해하는 경우에 이러한 고지의무를 면한다고 규정하고 있다.[98]

---

97) Article 29 Data Protection Working Party, Opinion 03/2013 on Purpose Limitation, 00569/13/EN WP203, 2 April 2013, p. 29.

둘째, 공익을 위한 기록보존, 과학 및 역사 연구, 통계 목적에 따른 개인정보 처리에 대하여 정보주체가 가지는 권리는 다음과 같이 제한된다. GDPR 제17조에 따른 삭제권은 해당 목적에 따른 개인정보의 처리를 불가능하게 만들거나 그러한 목적의 달성을 심각하게 저해하는 경우에 행사될 수 없다.[99] 또한 공익을 위한 기록보존, 과학 및 역사 연구, 통계 목적에 따른 개인정보 처리가 공적인 이유를 근거로 처리되는 경우에, 정보주체는 제21조에 따른 처리반대권을 주장할 수 없다.[100] 마지막으로 GDPR 제89조 2항은 공익을 위한 기록보존, 과학 및 역사 연구, 통계 목적에 따른 개인정보 처리에 대한 실효성을 확보하기 위하여, 동 규정 제15조, 제16조, 제18조에 따른 정보주체의 열람권, 정정권, 처리제한권의 행사를 유럽연합 또는 회원국의 입법조치로 제한할 수 있음을 규정하고 있다.[101]

셋째, GDPR 제9조 2항(j)에 따라 공익을 위한 기록보존, 과학 및 역사 연구, 통계 목적에 따른 민감정보 처리는 개인정보보호 권리의 본질을 존중하고, 그러한 목적이 비례적인 한도 내에서 허용된다.[102]

---

98) GDPR Art. 14. 5. Paragraphs 1 to 4 shall not apply where and insofar as: ... (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;

99) GDPR Art. 17. 3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary: (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.

100) GDPR Art. 21. 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.

101) GDPR Art. 89. 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 fulfillment of those purposes.

102) GDPR Art. 9. 2. Paragraph 1 shall not apply if one of the following applies: ... (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

이처럼 GDPR은 공익을 위한 기록보존, 과학 및 역사 연구, 통계 목적에 따른 개인정보 처리에 있어서 개인정보 활용의 유연성과 신축성을 대폭 확대하는 한편, 프로파일링을 포함한 자동화된 방식에 따른 개인정보 처리의 위험성을 자각하고 정보주체의 권리를 보호하는 관련 규정도 마련하고 있는데, 이는 후술한다.

### 1.3. 익명처리와 가명처리

GDPR은 익명처리와 가명처리를 명확히 구분하고 가명처리(pseudonymisation) 및 가명처리정보라는 새로운 개념을 도입하여, 정보주체의 권리를 보호하는 동시에 개인정보 활용의 신축성을 제고하고 있다. 다시 말해, GDPR은 가명처리와 가명처리정보를 GDPR의 적용범위에 포섭시키는 동시에, 개인정보처리자가 가명처리정보를 활용하도록 관련 규정을 완화시키고 있는 것이다. 이에 따라 개인정보처리자는 최초 수집 목적과 다른 추가 목적 또는 공익을 위한 기록보존, 과학 및 역사 연구, 통계 목적에 따라 '개인정보'에 해당하는 가명처리정보를 빅 데이터 분석에 활용할 수 있다.

#### 1.3.1. 익명처리정보와 가명처리정보의 법적 취급

익명처리(anonymisation) 및 가명처리(pseudonymisation)에 대한 개념을 살펴보기에 앞서, 1995년 개인정보보호지침이 GDPR로 대체되는 과정에서 두 개념의 지위가 어떻게 바뀌었는지를 살펴볼 필요가 있다. 먼저, 1995년 개인정보보호지침은 가명처리를 언급하고 있지 않다. 제29조 작업반은 '익명처리 기법에 관한 05/2014 의견' (Opinion 05/2014 on Anonymisation Techniques)에서 동 지침 해설전문 26항에 근거하여 익명처리의 개념을 설명하면서, 익명처리는 개인정보의 추가처리(further processing)로서 이해되어야 한다고 판단하였다.[103] 동 의견에서 가명처리는 1995년 개인정보보호지침에서 규정하고 있는 익명처리에 대한 오해(misconception)를 바로잡기 위한 비교대상으로서 부분적으로 논의되었다. 제29조 작업반은 가명처리가 익명처리의 수단이 아니라고 밝혔는데, 이는 가명처리정보가 재식별될 수 있는 위험이 아

rights and the interests of the data subject.

103) Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, 0829/14/EN WP216, 10 April 2014, p. 7.

주 작더라도 존재하기 때문이다.[104] 이러한 맥락에서, 제29조 작업반은 가명(pseudonymity)은 식별성(identifiability)을 허용할 가능성이 있으므로, 개인정보보호의 법체제의 범위 내에서 규율되어야 한다는 의견을 제시하였다.[105]

이와 달리, GDPR은 정의조항 제4조를 포함한 여러 관련 조항에서 가명처리를 상세히 규정하는 한편, 해설전문 26항을 통하여 익명처리정보와 익명처리정보의 처리는 동 규정의 적용 대상이 아님을 명시하고 있다.[106] 다시 말해, 1995년 개인정보보호지침이 GDPR로 대체되는 과정에서 비식별화조치와 관련된 주된 규율의 관심은 익명처리에서 가명처리로 바뀌었다 할 수 있다.

### 1.3.2. 개념

GDPR에서 가명처리와 익명처리에 대한 각각의 개념을 살펴보면 다음과 같다. 먼저 GDPR 제4조에 따라 가명처리는 개인정보의 처리에 해당하며, 가명처리된 개인정보는 여전히 개인정보로서 동 규정의 적용을 받는다. 여기서 가명처리란 추가적인 정보의 결합이 없을 때, 개인정보를 특정 정보주체에게 귀속시킬 수 없도록 처리하는 기법이다. 이러한 경우 개인의 식별을 가능케 하는 추가적인 정보는 별도로 보관되어야 하며, 해당 개인정보가 정보주체와 연결될 수 없도록 기술적·관리적 조치가 취해져야 한다.

> *Article 4 Definitions*
>
> (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;

익명처리에 대한 개념을 설명하고 있는 GDPR 해설전문 26항에 따르면, GDPR은 1) 식별된 또는 식별가능한 자연인(natural person)과 관련되지 않거나 2) 정보주체(data subject)를 더 이상 식별할 수 없도록 개인정보에 익

104) Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, 0829/14/EN WP216, 10 April 2014, p. 3.
105) Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, 0829/14/EN WP216, 10 April 2014, p. 10.
106) GDPR Recital (26).

명처리가 가해진 익명처리정보(anonymous information)에는 적용되지 않는다. 자연인에 대한 식별 가능성 여부를 판단하기 위해서는 정보처리자 또는 제3자에 의하여 합리적으로 사용될 것으로 예상되는 모든 수단이 고려되어야 하며, 그러한 수단이 합리적으로 사용될 것으로 예상되는지를 판단하기 위해서는 식별하기 위해 소요되는 비용·시간 등 객관적인 요소와 함께 처리 당시 가용한 기술과 기술적 발전을 모두 고려하여야 한다.[107]

> GDPR Recital (26)
>
> ...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.

익명처리와 가명처리에 대한 개념을 보다 자세히 이해하기 위하여, 국제표준화기구(International Organization for Standardization, 이하 ISO)의 의료정보 보호를 위한 기술보고서(ISO/TS 25237:2008)를 살펴보면 다음과 같다.[108] 동 보고서는 비식별처리(de-identification)를 '정보주체와 식별하는 개인정보셋 사이의 연결을 제거하는 과정의 일반용어 (general term for any process of removing the association between a set of identifying data and the data subject)'로 정의하고 있다.[109] 익명처리(anonymization)는 이러한 비식별처리의 하부범주로서, '정보주체와 식별하는 데이터셋 사이의 연결을 제거하는 과정(process that removes the association between the identifying dataset and the data subject)'이다.[110]

---

107) GDPR Recital (26) (...To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments...)

108) 동 보고서는 익명성의 기본 개념을 정의하고 비식별처리에 따른 개인정보 활용 사례를 설명하고 있다.

109) ISO/TS 25237:2008 Health informatics – Pseudonymization, p. 3; Simson L. Garfinkel, *De-Identification of Personal Information* 2 (NISTIR 8053, October 2015)에서 재인용.

110) ISO/TS 25237:2008 Health informatics – Pseudonymization, p. 2; Simson L. Garfinkel, *De-Identification of Personal Information* 2 (NISTIR 8053, October 2015)에서 재인용.

다음으로 ISO는 가명처리(pseudonymization)를 '정보주체와의 연결을 제거하고 또한 정보주체에 관련되는 특별한 특징셋과 하나 이상의 가명 사이의 연결을 추가하는 특별한 유형의 익명처리 (a particular type of anonymization that both removes the association with a data subject and adds an association between a particular set of characteristics relating to the data subject and one or more pseudonyms)'라고 정의하고 있다.[111] 일반적으로 가명처리는 직접 식별자를 무작위로 생성된 가치와 같은 가명(pseudonym)으로 대체되며,[112] 이때 가명(pseudonym)이란 '일반적으로 이용되는 개인 식별자와 다른 개인 식별자(personal identifier that is different from the normally used personal identifier)'를 의미한다.[113]

가명처리의 개념을 이해하기 위하여 직접 식별자(direct identifier)와 간접 식별자 (indirect identifier)를 구별하는 것은 중요한 문제이다. 직접 식별자와 간접 식별자를 정의하고 있는 ISO 보고서에 따르면, '한 개인을 직접적으로 식별하는 데이터 (개인정보) (data that directly identifies a single individual)'에 해당하는 직접 식별자는 '추가적 정보 없이 또는 공역에 있는 다른 정보를 통하여 교차연계하여 사람을 식별하는데 이용될 수 있는 데이터 (data that can be used to identify a person without additional information or with cross-linking through other information that is in the public domain)'이다.[114] 직접 식별자의 예는 이름, 사회보장번호나 이메일주소를 포함한다.[115] 간접 식별자는 '독립적으로 개인을 식별하지 않지만 추가적 데이터포인트와 결합한다면 개인 신원을 드러낼 수 있는 데이터 (data that do not identify an individual in isolation but may reveal individual identities if combined with additional data points)'에 해당한다. 예컨대, 생

111) ISO/TS 25237:2008 Health informatics – Pseudonymization, p. 5; Simson L. Garfinkel, *De-Identification of Personal Information* 2 (NISTIR 8053, October 2015)에서 재인용. 미국 NIST는 'anonymization' 대신 'de-identification'이라고 한다. Id., 43.

112) Simson L. Garfinkel, *De-Identification of Personal Information* 43 (NISTIR 8053, October 2015).

113) ISO/TS 25237:2008 Health informatics – Pseudonymization, p. 5; Simson L. Garfinkel, *De-Identification of Personal Information* 43 (NISTIR 8053, October 2015)에서 재인용.

114) ISO/TS 25237:2008 Health informatics – Pseudonymization, p. 3; Simson L. Garfinkel, *De-Identification of Personal Information* 15 (NISTIR 8053, October 2015)에서 재인용.

115) Simson L. Garfinkel, *De-Identification of Personal Information* 15 (NISTIR 8053, October 2015). 미국 HIPAA 프라이버시규칙 (HIPAA Privacy Rule)은 이름, 전화번호, 이메일주소 등의 고유 식별번호 등 18개 데이터유형을 직접 식별자로 규정한다. Id., 23-24.

일, 성별 및 우편번호라는 세 가지 간접 식별자를 결합하는 경우, 미국인의 87.1%가 식별될 수 있다고 한다.[116] 즉, 생일과 같은 간접 식별자를 단독으로 이용하여 개인을 식별하는 것은 어렵다하더라도, 성별과 우편번호라는 다른 간접 식별자를 결합하는 방식으로 특정 개인을 알아볼 수 있게 되는 것이다.

가명처리는 이러한 직접 식별자 및 간접 식별자를 제거하거나 모호하게 하는 것이다. 이들 데이터포인트는 무작위 식별 번호나 다른 가명과 같은 키를 사용하여 비식별화된 데이터베이스에 연계될 수 있는 별개의 데이터베이스에 보관된다. 익명처리와 달리, 가명처리는 추가적인 정보와의 결합을 통하여 개인을 재식별할 수 있는 위험성을 가지므로,[117] 그러한 위험성을 감소시키기 위하여 개인정보처리자는 '가명화의 허가받지 않은 가역 (unauthorized reversal of pseudonymization)'을 방지하는 적절한 안전조치를 이행하여야 한다.[118] 이러한 안전조치에는 암호화·해싱 (hashing)[119]·토큰화(tokenization)[120]와 같은 기술적 조치와,[121] 협약·정책·프라이버시 중심 설계 (privacy by design)와 같은 관리적 조치가 포함된다.[122]

### 1.3.3. 가명처리 관련 규정

GDPR은 다음과 같은 규정에서 가명처리를 규율하고 있다. 첫째, GDPR은 정보주체의 위험을 감소시키고 개인정보처리자의 의무를 충족시키는 기술적 조치로서 가명처리를 장려하고 있다.[123] 둘째, 가명처리정보를 어떠한 승인 없이 식별가능한 개인정보로 가역(reversal)하는 행위는 금지되며,[124] 이러한

---

116) Latanya Sweeney, "Simple Demographics Often Identify People Uniquely, Data Privacy Working Paper 3, 16 (Carnegie Mellon University. Pittsburgh 2000).

117) Gabe Maldoff, Top 10 operational impacts of the GDPR: Part 8 - Pseudonymization, Feb 12, 2016, https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-8-pseudonymization/.

118) GDPR, Recital 75.

119) '해시 (hash)'는 잘게 자른 조각을 의미하는데, 전산 처리에서 '해싱 (hashing)'은 디지털 숫자열을 원래의 것을 상징하는 더 짧은 길이의 값이나 키로 변환하는 것을 의미한다. 기록학용어사전, http://terms.naver.com/entry.nhn?docId=441307&cid=42081&categoryId=42081.

120) 토큰화는 모바일 결제 시스템에서, 신용카드와 같은 개인 정보를 보호하기 위해 관련 정보를 토큰으로 변환하여 사용하는 방식을 의미한다. IT용어사전, http://terms.naver.com/entry.nhn?docId=3377367&cid=42346&categoryId=42346.

121) Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, 0829/14/EN WP216, 10 April 2014, pp. 20-21.

122) Gabe Maldoff, Top 10 operational impacts of the GDPR: Part 8 - Pseudonymization, Feb 12, 2016, https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-8-pseudonymization/.

123) GDPR Recital (28), (29).

행위는 개인정보의 침해(personal data breach)를 구성한다.[125] 셋째, 전술한 바와 같이, 가명처리를 포함한 안전조치(safeguards)는 최초 수집 목적과 다른 목적의 양립 가능성을 판단하는 고려사항이다.[126] 넷째, 개인정보처리자는 개인정보보호 중심 디자인 및 설정(data protection by design and by default)을 고려하여, 처리의 방법을 결정하는 시점과 처리 당시 시점에서 가명처리를 포함한 안전조치를 취하여야 한다.[127] 다섯째, 개인정보처리자 및 수탁처리자는 개인정보의 안전한 처리(security of processing)를 위하여 기술적·관리적 조치의무를 가지는 바, 가명처리는 이러한 기술적 조치에 해당한다.[128] 여섯째, 개인정보처리자를 대표하는 협회나 기타 단체는 행동강령(code of conduct)을 제정함에 있어서 가명처리에 관한 세부규정을 마련할 수 있다.[129] 마지막으로, 가명처리는 공익을 위한 기록보존, 과학 및 역사 연구, 통계 목적에 따른 개인정보 처리에서 반드시 요구되는 안전조치(safeguards)의 예로서 명시적으로 언급되고 있다.[130]

특히, GDPR은 개인정보를 보유하고 있는 개인정보처리자로 하여금 자체적인 가명처리에 따른 개인정보의 활용을 허용하고 있다. 해설전문 29항은 이를 명시적으로 언급하고 있는데, 이에 따르면 개인정보처리자는 1) 개인을 식별하는데 쓰이는 추가정보를 별도로 보관하고, 2) 동 규정의 이행을 위하여 필요한 기술적·관리적 조치를 취하고, 3) 이를 감독하는 책임자를 선정하는 경우, 자신이 보유한 개인정보를 스스로 가명처리할 수 있다. 예를 들어, 오픈데이터를 통하여 수집한 식별가능한 개인정보나 제3자로부터 제공받은 개인정보를 가명처리한 후, 해당 가명처리정보를 통계 목적에 근거하여 빅데이터 분석에 이용하는 것은 GDPR에서 허용되는 것이다.

*GDPR Recital (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

124) GDPR Recital (75).
125) GDPR Recital (85).
126) GDPR Art. 6. 4.
127) GDPR Art. 25.
128) GDPR Art. 32.
129) GDPR Art. 40.
130) GDPR Art. 89.

| |
|---|
| 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. |

## 2. 개인정보보호법

### 2.1. 개인정보의 목적 외 이용·제공

GDPR 제5조와 마찬가지로 개인정보보호법은 제3조에서 개인정보 처리 목적을 명확하게 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 처리해야함을 원칙으로 규정하고 있다. 그러나 개인정보의 활용을 허용할 수 있는 목적 외 처리 규정과 관련하여 개인정보보호법은 다음과 같은 차이점을 가지고 있다.

첫째, 개인정보보호법은 제2조에서 처리를 “개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그밖에 이와 유사한 행위”로 정의하고, 제18조의 적용범위를 처리 가운데 이용·제공에 국한하였다.[131] 이는 개인정보보호법이 수집(제15조), 제공(제17조), 파기(제21조) 등 특정 유형의 개인정보 처리를 각각의 조항에서 개별적으로 규율하고 있기 때문이다. 물론, 빅 데이터 분석, 오픈 데이터를 이용한 개인정보의 활용은 대개의 경우 개인정보의 이용·제공에 해당한다 하겠으나, 개인정보의 목적 외 수집·저장·보유·가공·편집 등이 허용되지 않는다는 점은 개인정보의 활용을 저해하는 결과를 야기할 수도 있다.

둘째, 개인정보보호법 제18조에 따라 동 법 제15조 및 제17조의 범위를 초과한 개인정보의 이용 및 제공은 원칙적으로 금지되지만, 이에 대하여 다음과 같은 예외사유가 존재한다.

[표 3-1] 개인정보의 목적 외 제공·이용에 대한 예외

| | |
|---|---|
| 제18조 | 1. 정보주체로부터 별도의 동의를 받은 경우<br>2. 다른 법률에 특별한 규정이 있는 경우 |

131) 개인정보보호법 제2조.

| | |
|---|---|
| 제2항 | 3. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우<br>4. 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우<br>5. 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우 (공공기관에 한함)<br>6. 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우 (공공기관에 한함)<br>7. 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우 (공공기관에 한함)<br>8. 법원의 재판업무 수행을 위하여 필요한 경우 (공공기관에 한함)<br>9. 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우 (공공기관에 한함) |
| 제58조 제1항 | 1. 공공기관이 처리하는 개인정보 중 「통계법」에 따라 수집되는 개인정보<br>2. 국가안전보장과 관련된 정보 분석을 목적으로 수집 또는 제공 요청되는 개인정보<br>3. 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우로서 일시적으로 처리되는 개인정보<br>4. 언론, 종교단체, 정당이 각각 취재·보도, 선교, 선거 입후보자 추천 등 고유 목적을 달성하기 위하여 수집·이용하는 개인정보 |

[표 3-1]에서 나타나는 바와 같이, 개인정보보호법은 목적 외 이용·제공에 대한 예외사유를 한정적으로 명시하고 있다. 이는 최초 수집 목적과 양립 가능한 목적에 따른 추가처리를 별도의 법적근거 없이 허용하고 있는 GDPR과 대조된다.

공익을 위한 기록보존, 과학 및 역사 연구, 통계적 목적에 근거한 목적 외 처리를 규정하는 GDPR과 유사하게, 개인정보보호법 제18조 2항 4호는 “특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우”를 요건으로, “통계작성 및 학술연구 등의 목적”에 따른 목적 외 이용 및 제공을 허용하고 있다. 결국 정보주체의 동의를 구하지 아니한 개인정보의 활용은 동 법 제18

조 2항 4호에 근거한다고 보는 것이 타당하므로, 빅 데이터 분석, 오픈 데이터 활용에 대한 허용여부는 1) 개인정보의 활용 목적이 통계작성 및 학술연구 등의 목적에 해당하는지 여부와 2) 특정 개인을 알아볼 수 없는 형태로 개인정보가 제공되었는지에 대한 여부에 따라 판단된다 할 수 있겠다.

### 2.2. 통계작성 및 학술연구 목적

개인정보보호법은 통계작성 및 학술연구의 개념과 범위에 대한 별도의 정의를 내리지 않고 있다. 다만 "통계작성 및 학술연구 등"이라는 문언에 따라 비단 통계와 연구 목적이 아니라하더라도 제18조 2항 4호의 취지에 부합하는 추가적인 개인정보 처리의 유형이 존재할 수 있다 하겠다.

GDPR과 비교하여, 통계작성 및 학술연구 목적에 따른 목적 외 제공·이용에는 다음과 같은 차이점이 존재한다. 첫째, 개인정보보호법 제18조 2항 4호는 "특정 개인을 알아볼 수 없는 형태로 개인정보를 제공"할 것을 특별히 요구하고 있다. 이와 달리, GDPR 제89조 1항은 공익을 위한 기록보존, 과학 및 역사 연구, 통계 목적에 따른 개인정보 처리에 있어서 적절한 안전조치(appropriate safeguards)가 반드시 확보되어야 함을 규정하고 있으며, 가명처리(pseudonymisation)는 이러한 안전조치에 포함된다.

> *Article 89 Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes*
>
> 1. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in 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.

둘째, 개인정보보호법은 제18조 2항 4호 외에 어떠한 조항에서도 통계작성 내지 학술연구 목적과 관련되는 규정을 마련하고 있지 않다. 다시 말해, 개인정보보호법은 제18조 내에서 목적 외 제공을 가능케 하는 예외사유로서

통계작성 및 학술연구 목적을 규정할 뿐, 이와 관련된 다른 조항을 구비하고 있지 않다. 이와 달리, GDPR에서 공익을 위한 기록보존, 과학 및 역사 연구, 통계 목적에 따른 목적 외 처리는 개인정보의 활용이라는 측면에서 법률 체계 전반에 반영되어 있다 하겠다.

## 3. 미국 및 일본 개인정보보호법제

빅 데이터 분석을 허용하는 방식에는 크게 두 가지 방식이 존재한다 할 수 있다. 첫 번째 방식은 개인정보를 최초 수집 시 목적이 아닌 추가 목적에 따라 목적 외 처리하도록 허용하는 방식으로, 앞서 살펴본 GDPR이 취하고 있는 방식이다. 두 번째 방식은 개인정보를 비식별처리하여 해당 정보를 더 이상 개인정보로 취급하지 않음으로써, 그러한 비식별처리정보의 빅 데이터 활용을 관련 개인정보보호법제의 적용범위에서 배제하는 방식이다. GDPR은 가명처리정보와 익명처리정보를 구분하여, 개인정보에 해당하는 가명처리정보는 일정한 법률요건을 충족하는 경우 목적 외 처리로서 허용하고, 개인정보에 해당하지 않는 익명처리정보의 활용은 GDPR의 적용을 배재함으로써 상기 두 가지 접근 방식을 모두 취한다고 볼 수 있다.[132)]

이와 달리, 미국의 '비식별정보(de-identified data)'와 '비식별건강정보(de-identified health data)', 일본의 '익명가공정보'는 개인정보에 해당하지 않는 정보로서 자유로운 이용 및 제공이 가능한 바, 두 국가는 빅 데이터 분석 등 개인정보의 활용을 위하여 후자의 접근 방식을 취하고 있는 것으로 보인다. 다시 말해, 이러한 비식별 조치에 따른 빅 데이터 분석의 허용은 관련 개인정보보호법제의 테두리 안에서 규율되는 것이 아니라, 그러한 법의 적용범위를 벗어나 허용되는 것이다.

### 3.1. 미국의 비식별정보(de-identified data) 및 비식별건강정보(de-identified health data)

#### 3.1.1. 소비자 프라이버시 권리 장전 행정논의초안

132) GDPR Recital (26).

미국은 한국, 유럽연합, 일본과 달리 개인정보를 규율하는 일반법이 존재하지 않는다. 온라인 개인정보 처리에 관하여 소비자의 프라이버시 권리를 확립하기 위한 목적으로 2012년 오바마 행정부가 제안한 '소비자 프라이버시 권리 장전(Consumer Privacy Bill of Rights)'은 아직까지 의회에서 통과되지 못하고 있는 실정이다. 다만, 소비자 프라이버시 권리 장전 행정논의초안(Administration Discussion Draft)은 제4조 (a)에서 개인정보를 정의하는 한편, 개인정보의 예외(exception)로서 비식별정보(de-identified data)를 다음과 같이 정의하고 있다.

> SEC. 4. Definitions.
> (1) Personal Data. (...)
> (2) Exceptions.
> (A) De-identified data.—The term "personal data" shall not include data otherwise described by paragraph (1) that a covered entity (either directly or through an agent)—
>
> (i) alters such that there is a reasonable basis for expecting that the data could not be linked as a practical matter to a specific individual or device;
> (ii) publicly commits to refrain from attempting to identify with an individual or device and adopts relevant controls to prevent such identification;
> (iii) causes to be covered by a contractual or other legally enforceable prohibition on each entity to which the covered entity discloses the data from attempting to link the data to a specific individual or device, and requires the same of all onward disclosures; and
> (iv) requires each entity to which the covered entity discloses the data to publicly commit to refrain from attempting to link to a specific individual or device.

이에 따르면, 개인정보처리자(covered entity)[133]가 ① 특정 개인 또는 기기(device)와 정보가 실질적으로 연결될 수 없다는 사실을 기대할 수 있을 만큼의 합리적인 근거로 정보를 변형(alter)하고, ② 개인 또는 기기를 식별하

133) 초안에서 정의하는 'covered entity'란 개인정보를 주간 상업(interstate commerce)에서 수집, 형성, 처리, 보관, 이용 또는 공개하거나 주간 상업에 영향을 끼치는 개인정보를 수집, 형성, 처리, 보관, 이용 또는 공개하는 자를 의미한다. 이는 개인정보보호법의 개인정보처리자, GDPR의 'data controller'와 유사한 개념이다. 각각의 용어는 그 개념이 완벽히 일치하지는 않으나, 이하에서는 서술의 편의를 위하여 'covered entity'를 개인정보처리자로 서술한다. Consumer Privacy Bill of Rights Administration Discussion Draft, SEC. 4. (b) "Covered entity" means a person that collects, creates, processes, retains, uses, or discloses personal data in or affecting interstate commerce.

는 시도를 하지 않을 것을 공개적으로 약속하고, 그러한 식별을 예방하기 위하여 관련된 통제(control)를 하고, ③ 개인정보가 공개된 다른 개인정보처리자로 하여금 특정 개인 또는 기기와 개인정보를 연결하도록 시도하는 것을 계약적으로 또는 법률적으로 금지시키고, 향후 정보의 제공에 있어서도 이러한 식별의 금지를 요구하고, ④ 개인정보가 공개된 다른 개인정보처리자로 하여금 해당 정보와 개인 또는 기기를 연결하지 않을 것을 공개적으로 약속할 것을 요구하는 경우, 해당 정보는 비식별정보가 된다.

소비자 프라이버시 권리 장전 행정논의초안에 따라 비식별처리가 이루어진 비식별정보(de-identified data)는 개인정보에 해당하지 않는다. 따라서 빅 데이터 분석에 있어서 비식별정보의 활용은 GDPR의 익명처리정보와 유사하게 개인정보보호법제 적용 범위 밖에서 허용된다 하겠다. 이러한 비식별정보는 개인뿐만 아니라 휴대폰, 태블릿 등과 같은 기기(device)의 고유 디바이스 번호 등을 포함하고 있다.

### 3.1.2. HIPAA 프라이버시 규칙

비식별처리(de-identification)에 따른 개인정보의 처리를 허용하고 있는 개별 법령으로서 '건강보험 이전과 책임에 관한 법(Health Insurance Portability and Accountability. 이하 HIPAA)'에 근거하여 미국 보건복지부가 발행한 'HIPAA 프라이버시 규칙(HIPAA Privacy Rule)'이 존재한다.[134]

동 규칙의 보호대상은 '건강정보(Protected Health Information, 이하 PHI)'로서, 이는 의료서비스제공자(health care providers) 등 동 규칙에 따라 건강정보 보호의무를 가지는 개인정보처리자(covered entity)에 의하여 보유되거나 전송되는 '개별적으로 식별 가능한 건강정보(individually identifiable health information)'를 의미한다.[135] 여기서 '개별적으로 식별 가능한 건강정보'라 함은 ① 개인의 과거, 현재 또는 미래의 신체적·정신적 건강 또는 상태

134) HIPAA는 동 법률이 발효된 이후 3년 이내에 미국 의회가 프라이버시 관련 법률을 입법하지 않는 경우, 보건복지부 장관으로 하여금 개인을 알아볼 수 있는 건강정보에 대한 관련 프라이버시 규정을 공표할 것을 요구하고 있다. 이에 따라 HIPAA 프라이버시 규칙은 HIPAA가 발효된 후 상기 기간동안 의회가 관련 입법을 채택하지 않았음을 근거로 보건복지부에 의하여 발행된 규정으로 미국연방규정집(Code of Federal Regulations) 제160부(Part 160) 및 제164부(Part 164)에 수록되어 있다.

135) 45 C.F.R. § 160.103.

(condition), ② 개인에 대한 의료서비스의 제공, ③ 개인에 제공된 의료서비스의 과거, 현재 또는 미래의 납입내역(payment)과 관련하여 1) 개인을 식별할 수 있는 정보 또는 2) 합리적인 이유에 의하여 개인을 식별하기 위하여 이용될 것이라 믿을 수 있는 정보를 의미한다.[136] 개별적으로 식별 가능한 개인정보는 이름, 주소, 생년월일, 사회보장번호(Social Security Number) 등 여러 식별인자를 포함한다. 다만, '가족 교육권 및 프라이버시에 관한 법률(Family Educational Rights and Privacy Act)'의 적용을 받는 근로기록(employment records) 등은 HIPAA 프라이버시 규칙의 적용을 받지 않는다.[137]

HIPAA 프라이버 규칙은 개인의 PHI가 어떠한 상황에서 이용되거나 공개될 수 있는지에 대하여 관련 기준을 정하고 이를 제한하는데 주된 목적이 있다. 동 규칙에 따라 개인정보처리자는 첫째, 동 규칙이 허용하거나 요구하는 경우, 또는 둘째, 해당 정보의 대상이 되는 개인(정보주체와 유사한 개념) 또는 그의 대리인이 서면 형식으로 승인하는 경우에 한하여 PHI의 처리를 할 수 있다.[138]

또한 의료정보처리기관은 ① 개인 또는 그의 대리인이 해당 개인의 PHI에 대하여 접근을 요구하는 경우 이를 공개해야하며, ② 조사·검토·법 집행과 관련된 의무 준수를 위하여 필요한 경우 해당 정보를 보건복지부에 공개해야만 한다.[139] PHI의 의무적 공개는 오직 상기 두 경우에만 국한된다.

HIPAA 프라이버 규칙에 따라 비식별건강정보(de-identified health information)의 이용 또는 공개에는 어떠한 제한도 존재하지 않는다.[140] 비식별정보는 다음의 두 가지 경우에 제한적으로 인정된다. 첫째, 통계 및 과학 분야에 있어서 적절한 지식을 갖추고 있는 전문가가 ① 통계·과학 원칙 및 방법(statistical and scientific principles and methods)을 적용하여 비식별처리를 감행하고, 해당 정보가 예견된 수령인에 의하여 단독적으로 또는 합리적으로 이용 가능한 또 다른 정보와의 결합을 통하여 식별될 수 있는 위험

136) 45 C.F.R. § 160.103.
137) Family Educational Rights and Privacy Act, 20 U.S.C. §1232g.
138) 45 C.F.R. § 164.502(a).
139) 45 C.F.R. § 164.502(a)(2).
140) 45 C.F.R. §§ 164.502(d)(2), 164.514(a) and (b).

성이 '매우 적다 (very small)'고 판단한 후, ② 그러한 판단을 정당화하는 비식별처리 및 그에 따른 결과에 대한 분석을 문서로 작성하는 경우이다.[141] 'PHI 비식별처리 가이드 (Guidance on De-identification of Protected Health Information)'에 따라 이러한 비식별처리 방식을 '전문가 결정방식 (Expert Determination Method)'이라고 부른다.

> 45 C.F.R. § 164.514
>
> (b) Implementation specifications: requirements or de-identification of protected health information. A covered entity may determine that health information is not individually identifiable health information only if:
>
> (1) A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable: (i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information identify an individual who is a subject of the information; and (ii) Documents the methods and results of the analysis that justify such determination.

둘째, 개인 또는 개인의 친척, 고용주, 가족구성원에 관한 총 18가지의 식별인자(identifiers)[142]을 제거하고, 개인정보처리자가 식별인자가 제거된 정보를

141) 45 C.F.R. § 164.514(b)(1). (i)A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable: Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information identify an individual who is a subject of the information; and (ii) Documents the methods and results of the analysis that justify such determination.

142) 45 C.F.R. § 164.514(b)(2)(i) The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed: (A) Names; (B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000. (C) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older; (D) Telephone numbers; (E) Fax numbers; (F) Electronic mail addresses; (G) Social security numbers; (H) Medical record numbers; (I) Health plan beneficiary numbers; (J) Account numbers; (K) Certificate/license numbers; (L) Vehicle identifiers and serial numbers, including license plate numbers; (M) Device identifiers and serial numbers; (N) Web Universal Resource Locators (URLs); (O) Internet Protocol (IP) address numbers; (P) Biometric identifiers,

단독적으로 또는 이용 가능한 다른 정보와의 결합을 통하여 개인을 식별할 수 있는 실질적 지식 (actual knowledge)을 가지고 있지 않은 경우, 해당 정보는 비식별정보가 된다.[143] 상기 18가지 식별인자는 ① 이름, ② 주소정보, ③ 개인과 직접 관련된 날짜정보(생일, 합격일 등), ④ 전화번호, ⑤ 팩스번호, ⑥ 이메일 주소, ⑦ 사회보장번호, ⑧ 의료기록번호, ⑨ 건강보험번호, ⑩ 계좌번호, ⑪ 자격취득번호, ⑫ 자동차번호, ⑬ 각종 장비 식별번호, ⑭ URL 정보, ⑮ IP주소, ⑯ 생체정보, ⑰ 전체 얼굴사진과 이와 유사한 이미지, ⑱ 기타 특이한 식별 번호 또는 코드가 존재한다. 이러한 비식별처리 방식을 '세이프 하버 방식 (Safe Harbor Method)'이라 한다.

## 3.2. 일본의 익명가공정보

### 3.2.1 특정 이용목적을 위한 개인정보의 취급

일본의 개정 개인정보보호법[144] 에 따라 개인정보를 취급하는 개인정보취급사업자는 개인정보의 이용목적을 가능한 한 특정하여야 한다. 이용목적을 변경하는 경우에는 변경 전 이용목적과 관련성이 있다고 합리적으로 인정되는 범위를 초과해서는 안 된다.[145] 개정 전 법률에서는 변경 전 이용목적과 '상당한' 관련성을 요구하였으나, 개정법에서 동 문언이 삭제되었다. 또한 원칙적으로 모든 이용 목적에 대하여 본인의 동의를 받아야 하며, 동의를 받지 않고 그 이용목적의 달성에 필요한 범위를 초과하여 개인정보를 취급하는 것은 금지된다.[146] 다만, 법령에 의거한 경우, 사람의 생명·신체·재산의 보호를 위해 필요한 경우로서 본인의 동의를 받기가 곤란한 경우, 공중위생의 향상 또는 아동의 건전한 육성 추진을 위해 특히 필요한 경우로서 본인의 동의를 받기가 곤란한 경우, 국가기관, 지방공공단체 또는 그 위탁을 받은 자가 법령에 정한 사무를 수행함에 있어 협력이 필요한 경우로서, 본인의 동의를 받도록 하면 당해 사무의 수행에 지장을 초래할 우려가 있는 경우에는

---

including finger and voice prints; (Q) Full face photographic images and any comparable images; and (R) Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section.

143) 45 C.F.R. § 164.514(b)(2)(ii) The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

144) 個人情報の保護に關する法律 (平成15年法律第57号)

145) 일본개인정보보호법 제15조.

146) 일본개인정보보호법 제16조1항.

예외로 한다.[147]

이처럼 일본 개인정보보호법은 개인정보의 목적 외 처리를 규정하고 있으나, 개인정보의 목적 외 이용 및 개인데이터의 제3자 제공에 대하여 정보주체의 동의를 받을 것을 의무화하고 있다. 당초에는 상정하지 않았던 새로운 이용목적이 발생하거나 예정되지 않았던 제3자 제공을 하는 경우에는, 해당되는 본인 전부로부터 동의를 받아야 하고, 이는 개인정보를 이용한 신규 사업을 저해하는 하는 상황으로 이어질 수 있다는 점이 지적되어 왔다.

### 3.2.2. 익명가공정보

일본 개인정보보호법에서 빅 데이터 분석 등 개인정보의 활용은 목적 외 처리 규정이 아니라 '익명가공정보' 규정에 의하여 허용되고 있다. 개인정보에 해당하지 않도록 데이터를 가공하여 '익명화'함으로써 정보주체의 프라이버시를 보호하면서 활용이 가능하도록 하고, 이와 같이 가공된 정보를 '익명가공정보'로서 새로이 정의하여, 정보주체의 동의 없이도 해당 정보를 이용하고 제공할 수 있는 제도를 마련한 것이다.[148]

익명가공정보란, 특정 개인을 식별할 수 없도록 개인정보를 가공하여 얻어지는 개인에 관한 정보로서, 당해 개인정보를 복원할 수 없도록 만든 정보이다.[149] 즉 개인정보의 정의 각호에서 개인정보로서 식별되는 부분을 삭제하고 이를 복원할 수 없게 가공함으로써 익명성을 유지하도록 만든 것이다. 특정 익명가공정보를 컴퓨터를 이용하여 검색할 수 있도록 체계적으로 구성한 것을 사업의 용도로 취급하거나 제공하는 자는 익명가공정보취급사업자로서 의무를 부담하게 된다.[150]

---

147) 일본개인정보보호법 제16조3항.

148) 大場 敏行, 約10年ぶりの改正：新しい個人情報保護法とその影響 前編, デロイトトーマツサイバーセキュリティ先端研究所 ニュースレター Vol.4 (2016.1.22.).

149) 일본개인정보보호법 제2조9항. 익명가공정보란 다음의 각호에 해당하는 개인정보 구분에 대응하고 해당 각호에 정하는 조치를 취하여 특정 개인을 식별할 수 없도록 개인정보를 가공하여 얻는 개인에 관한 정보로서, 해당 개인정보를 복원할 수 없도록 한 것을 말한다. 1호. 제1항제1호에 해당하는 개인정보. 당해 개인정보에 포함된 기술 등의 일부를 삭제하는 것(당해 일부 기술 등을 복원할 수 있는 규칙성을 가지지 않은 방법에 의해 다른 기술 등으로 대체하는 것을 포함) 2호. 제1항제2호에 해당하는 개인정보. 당해 개인정보에 포함되는 개인식별부호의 전부를 삭제하는 것(당해 개인식별부호를 복원할 수 있는 규칙성을 가지지 않은 방법에 의해 다른 기술 등으로 대체하는 것을 포함).

150) 일본개인정보보호법 제2조10항 (익명가공정보취급사업자)익명가공정보를 포함하는 정보 집합물로서 특정 익명가공정보를 전자계산기를 이용하여 검색할 수 있도록 체계적으로 구성한 것 기타 특

일본 개인정보보호법의 개정을 검토하는 과정에서 특정 개인을 식별할 가능성을 감소시키기 위하여 가공을 하더라도 완전히 개인을 특정할 수 없는 정보로 가공하는 방법을 정하는 것은 어렵다는 점이 지적되어 왔다.[151] 때문에 익명가공정보는 특정 개인이 식별될 위험을 염두에 두고 가공한 정보로 평가되고 있으며, 그 적정한 취급을 위한 규칙이 다음과 같이 마련되어 있다.[152]

### 3.2.3. 익명가공정보 취급규칙

#### 3.2.3.1. 익명가공정보의 작성

익명가공정보 취급에 관한 절차로는 익명가공정보의 작성, 익명가공정보의 제공, 식별행위의 금지, 안전관리조치 등이 규정되어 있다. 먼저, 익명가공정보를 작성하는 경우에는 개인정보보호위원회규칙에 정하는 바에 따라 특정 개인을 식별할 수 없도록 하고, 그 작성에 사용된 개인정보를 복원할 수 없도록 당해 개인정보를 가공하여야 한다.[153] 익명가공정보를 작성한 때에는 개인정보보호위원회규칙에 정하는 기준에 따라, 가공방법에 관한 정보 유출을 방지하기 위해 필요한 대책으로서 이들 정보의 안전관리조치를 강구하여야 한다.[154] 또한 그 익명가공정보에 포함되는 개인정보의 항목을 공표하여야 한다. 그 취지는 익명가공정보를 작성한 후에도 특정 개인을 식별할 가능성이 완전히 없어지는 것은 아니므로, 제3자에게 제공하는 경우에 익명가공데이터에 포함되는 항목을 미리 공표함으로써 개인의 권익을 보호하고 투명성을 확보하는 것이 목적이다. 해당 항목으로는 거주지역, 연령, 구입상품명, 제공된 익명가공데이터의 종류와 포함된 사항 등을 들 수 있다. 익명가공정

---

정 익명가공정보를 용이하게 검색할 수 있도록 체계적으로 구성한 것으로서 정령으로 정한 것(제36조 1항의 익명가공정보데이터베이스등)을 사업용으로 제공하고 있는 자를 말한다.

151) 新保 史生, 個人情報保護法改正のポイントを學ぶ (7) : 匿名加工情報の取り扱い, 國民生活 (2016.4), p.26.

152) 일본개인정보보호법 제2절 익명가공정보취급사업자등의 의무. 2016년 6월 현재 일본 개인정보보호위원회는 익명가공정보의 가공방법과 안전관리 등에 관한 규칙을 제정하기 위하여 그 내용을 검토 중에 있다. 改正個人情報保護法の 概要と施行に向けた 取組について, 個人情報保護委員會事務局 (2016.6), pp.8-9.

153) 일본개인정보보호법 제36조(익명가공정보의 작성등) 1항. 익명가공정보 작성 시, 특정 개인을 식별하는 것과 그 작성에 이용되는 개인정보를 복원할 수 없도록 하기 위해 필요한 것으로서 개인정보보호위원회규칙에 정한 기준에 따라 당해 개인정보를 가공해야 한다.

154) 일본개인정보보호법 제36조6항.

보를 작성한 후에는 그 익명가공정보를 다른 정보와 조합하여 복원하는 것이 금지된다. 때문에 익명가공정보를 작성한 사업자 자신이 그 정보를 취급하는 경우에도, 익명가공정보의 작성에 사용된 개인정보에 관하여 본인을 식별하는 것은 허용되지 않는다.[155]

### 3.2.3.2. 익명가공정보의 제공

익명가공정보취급사업자가 익명가공정보를 제3자에게 제공하는 때에는, 제3자에게 제공되는 익명가공정보에 포함된 개인정보의 항목과 그 제공방법에 대하여, 개인정보보호위원회규칙에 정하는 사항을 공표하여야 한다. 또한 제공하는 정보가 익명가공정보라는 사실을 명시하여야 한다.[156]

### 3.2.3.3. 식별행위의 금지

익명가공정보를 작성한 사업자가 개인정보로 복원하는 것은 금지되며, 익명가공정보취급사업자는 식별행위 금지의무가 있다.[157] 완전한 익명가공정보를 작성 및 가공하는 방법을 정하는 것이 불가능한 현실에서, 일반적으로 공개된 정보와 기존에 보유하고 있는 정보를 취합하거나 분석함으로써 특정 개인을 식별할 수 있을 가능성이 있다. 이와 같은 처리를 의도적으로 시행하는 것은 금지되며. 의도하지 않게 식별되는 일이 없도록, 자신이 보유한 개인정보와 혼동하여 취급하지 않도록 주의가 필요하다.[158]

### 3.2.3.4. 안전관리조치

익명가공정보의 안전관리를 위해 필요하고 적절한 조치, 익명가공정보의 취급에 관한 고충 처리, 기타 익명가공정보의 적정한 취급을 확보하기 위하여

---

155) 일본개인정보보호법 제36조5항.

156) 일본개인정보보호법 제37조 (익명가공정보의 제공) 익명가공정보를 제3자에게 제공하는 경우에는 개인정보보호위원회 규칙에서 정하는 바에 따라, 제3자에게 제공되는 익명가공정보에 포함되는 개인에 관한 정보의 항목 및 그 제공 방법에 대하여 공표함과 동시에, 당해 제3자에 대해서 당해 제공에 관련된 정보가 익명가공정보임을 명시하여야 한다.

157) 일본개인정보보호법 제38조 (식별행위의 금지) 익명가공정보취급사업자는, 익명가공정보를 취급함에 있어 당해 익명가공정보의 작성이 이용된 개인정보에 관한 본인을 식별하기 위해서 당해 개인정보에서 삭제된 기술등 또는 개인식별부호 또는 제36조제1항의 규정에 의해 행해진 가공방법에 관한 정보를 취득하거나, 또는 당해 익명가공정보를 다른 정보와 조합(照合)해서는 안 된다.

158) 新保 史生, 個人情報保護法改正のポイントを學ぶ (7) :匿名加工情報の取り扱い, 國民生活 (2016.4), p.27.

필요한 조치를 강구하고, 당해 조치의 내용을 공표하도록 노력하여야 한다.[159] 익명가공정보는 그 가공방법 등이 공개되면 특정 개인에 대한 식별이 가능할 수 있는 정보이다. 때문에 그 취급에 관하여 안전관리조치를 모색하는 것이 필수적이며, 또한 종업원과 수탁업자에 대한 감독도 필요하다.

### 3.3. 비식별처리 정보에 대한 재식별 금지

미국과 일본의 관련 법제는 비식별정보, 비식별건강정보 및 익명가공정보를 개인정보로 보지 않는 한편, 개인정보의 완벽한 익명처리가 불가능하다는 인식아래, 이러한 비식별처리 정보의 가역 또는 재식별을 금지하는 규정을 함께 마련하고 있다. 소비자 프라이버시 권리 장전 초안의 경우, 개인정보처리자(covered entity)로 하여금 재식별 금지를 약속하도록 요구하거나, 수령인으로 하여금 비식별정보의 재식별을 금지하는 계약 또는 법률상의 의무를 부여하는 것은 그러한 비식별 처리 정보가 만에 하나 재식별될 수 있는 기술적 가능성을 염두하고 있기 때문으로 사료된다.

일본 개인정보보호법 역시 이와 유사한 맥락에서 익명가공정보의 재식별을 금지하고 있는 것으로 보인다. 다시 말해, 이미 익명가공정보를 '개인정보가 복원될 수 없도록 가공된 정보'라고 정의하고 있으면서도, 이러한 익명가공정보의 재식별을 금지하는 규정을 별도로 명시하고 있는 이유는, 개인정보의 완전한 익명처리가 현실적으로 불가능하다는 우려가 지속적으로 제기되고 있기 때문이다.

## 4. 빅 데이터 분석 활용을 위한 개인정보보호법 개정 방안

빅 데이터 분석을 포함한 개인정보의 활용을 도모하기 위하여 개인정보보호법은  첫째, GDPR의 목적 외 처리 및 가명처리 관련 규정을 반영할 수 있고, 둘째, 미국과 일본 개인정보보호법제에 따른 비식별 처리 규정을 반영할 수 있다 하겠다. 이에 대하여 각각의 경우를 살펴보면 다음과 같다.

159) 일본개인정보보호법 제39조 (안전관리조치등) 익명가공정보취급사업자는, 익명가공정보의 안전관리를 위해 필요하고 적절한 조치, 익명가공정보의 취급에 관한 고충 처리, 기타 익명가공정보의 적정한 취급을 확보하기 위하여 필요한 조치를 스스로 강구하고, 당해 조치의 내용을 공표하도록 노력해야 한다.

## 4.1. GDPR 목적 외 처리 규정을 반영하는 경우

GDPR의 목적 외 처리 및 가명처리 관련 규정을 반영하는 경우, 개인정보보호법은 제18조 목적 외 이용·제공에 관한 규정을 중심으로 다음과 같이 개정될 수 있다. 첫째, 개인정보보호법 제2조 정의조항에서 '가명처리'의 개념을 정의하고, 익명처리를 권고하는 제3조 7항 등 익명처리 관련 규정을 가명처리 관련 규정으로 재정비한다.

개인정보보호법 제2조에 따른 개인정보의 정의에 따라 익명처리정보는 개인정보에 해당하지 않는다. GDPR의 규정을 반영하는 경우, 가장 큰 장점은 빅데이터 분석을 촉진하고 장려하는 과정에서 가명처리정보에 대한 개인정보보호법의 규율이 여전히 적용될 수 있다는 점이다. GDPR이 기존 1995년 개인정보보호지침에는 존재하지 않았던 가명처리 규정을 도입한 이유 역시 개인정보보호와 개인정보의 활용이라는 두 보호법익을 법의 테두리 안에서 규율하기 위함이다. 가명처리를 GDPR의 적용범위에 포섭하였다는 사실은, 가명처리정보의 활용을 허용하는 한편, 개인정보처리자의 안전조치의무, 정보주체의 권리행사와 같은 일련의 개인정보보호 법원칙을 빅 데이터 분석에서도 적용 가능케 한다는 점에서 의미하는 바가 크다.

둘째, 목적 외 이용·제공을 허용하는 핵심 조항에 해당하는 개인정보보호법 제18조 2항 4호는 다음과 같은 방식으로 개정될 수 있다. 제시된 문구에 따르면, 개인정보처리자는 통계 및 연구 등 목적에 따라 자신이 보유하고 있는 개인정보를 스스로 가명처리하여 이를 활용하는 것이 허용된다.

> 제18조(개인정보의 목적 외 이용·제공 제한)
>
> ② 제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다. 다만, 제5호부터 제9호까지의 경우는 공공기관의 경우로 한정한다.
>
> **4. 통계 및 연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 가명처리하여 이용·제공하는 경우**

셋째, 개인정보처리자의 의무, 정보주체의 권리 등 가명처리에 대한 관련 규정을 재정비한다. 이러한 규정에는 ① 프로파일링 관련 규정, ② 가명처리에 관하여 개인정보처리자에게 부여되는 안전조치의무, ③ 가명처리정보의 불법적인 가역 또는 재식별화의 금지 및 처벌 등이 포함될 수 있다.

마지막으로 넷째, 개인정보의 이용 및 제공의 신축성을 확대하기 위하여, 개인정보보호법 제1조에 개인정보의 활용이라는 목적을 명시한다. 현행 개인정보보호법은 개인의 자유와 권리에 대한 보호만을 목적으로 천명하고 있는 바, 이에 더하여 개인정보의 활용에 따른 국민 편의, 복지 증진, 국가 경제 활성화의 도모를 개인정보보호법의 보호법익으로 삼을 필요가 있다.[160]

### 4.2. 미국 및 일본의 개인정보보호법제를 반영하는 경우

미국 및 일본의 법제를 반영한다면, 개인정보보호법은 다음과 같이 개정될 수 있다. 첫째, 정의조항에서 미국의 비식별정보(de-identified data) 또는 일본의 익명가공정보와 같이 비식별 조치가 취해진 정보를 별도로 정의한다. 둘째, 상기 정의된 비식별 정보는 개인정보에 해당하지 않는다는 사실을 명시하여, 해당 정보를 개인정보보호법의 적용 범위에서 배제시킨다. 셋째, 비식별 정보의 재식별화를 금지하는 관련 규정을 마련한다. 이러한 방식을 채택하는 경우, 빅 데이터 분석 등 개인정보의 활용은 개인정보에 해당하지 않는 비식별 처리 정보의 활용으로서 허용할 수 있다. 미국 및 일본의 법제를 반영하는 경우, 공익을 위한 기록보존, 과학 및 역사 연구, 통계의 목적으로 개인정보 활용의 범위를 제한하고 있는 GDPR과 달리 비식별 처리 정보의 활용 범위가 제한되지 않게 된다.

160) GDPR은 정보주체의 권리뿐만 아니라, 유럽연합 내의 개인정보의 자유로운 이동을 동 규정의 목적으로 함께 규정하고 있다. 대한민국 정보통신망법 역시 제1조에서 “정보통신망의 이용을 촉진하고 정보통신서비스를 이용하는 자의 개인정보를 보호함과 아울러 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성하여 국민생활의 향상과 공공복리의 증진에 이바지함”을 목적으로 천명하고 있다. 또한 신용정보보호법 제1조 역시 “이 법은 신용정보업을 건전하게 육성하고 신용정보의 효율적 이용과 체계적 관리를 도모하며 신용정보의 오용·남용으로부터 사생활의 비밀 등을 적절히 보호함으로써 건전한 신용질서의 확립에 이바지함을 목적으로 한다.”고 규정하는 바, 두 법은 개인정보보호와 마찬가지로 정보통신망 이용의 촉진, 신용정보의 효율적 이용을 법률이 보호하는 법익으로서 천명하고 있는 것이다.

# IV. 기타 주요 쟁점

## 1. 프로파일링

앞서 살펴본 바와 같이, GDPR은 목적 외 처리와 가명처리 규정을 근거로 과학·역사 연구 및 통계목적에 따른 빅 데이터 분석의 활용을 허용하고 있다. GDPR은 이처럼 빅 데이터 분석, 오픈 데이터 이용 등을 포함한 개인정보의 활용과 관련하여 규제를 완화하면서도, 대규모 자동화된 방식에 따른 개인정보 처리로 인하여 정보주체의 권리가 침해되는 것을 방지하기 위하여 관련 규정을 마련하고 있다.

우선, GDPR은 '프로파일링(profiling)'의 개념을 별도로 정의하고 있다. GDPR 제4조 (4)에 따르면, 프로파일링이란 정보주체의 개인적 측면(personal aspects)을 평가하기 위하여 -특히 개인의 업무능력, 경제 상황, 건강, 개인의 성향이나 관심사, 신뢰도, 행동, 위치, 이동에 관한 측면을 분석 및 예측하기 위하여 - 개인정보를 사용하는 자동화된 방식의 개인정보 처리를 의미한다.[161] 1995년 개인정보보호지침에는 프로파일링과 관련된 규정이 존재하지 않는다. 이러한 맥락에서, GDPR이 프로파일링 기법을 명시적으로 정의하고 이에 대한 관련 규정을 새롭게 도입하였다는 사실은, 빅 데이터 분석의 활용을 포함한 개인정보 처리 기술의 발전을 GDPR이라는 개인정보보호법제의 테두리 안에서 규율하고자 하는 입법의도를 나타내는 것이라 할 수 있다.

| *Article 4 Definition* |
| --- |
| (4) 'profiling'means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects |

161) GDPR Art. 4.

| |
|---|
| 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; |

## 1.1. 프로파일링 처리를 위한 요건

전술한 바와 같이, GDPR은 개인정보처리자로 하여금 정보주체의 권리와 자유에 대한 심각한 위험(high risk)을 초래할 가능성이 높은 유형의 개인정보 처리에 대하여 DPIA를 시행할 것을 요구하고 있으며, 이러한 평가의 목적은 개인정보가 처리되기 이전에 해당 정보의 처리의 위험성을 사전에 예측하기 위함이다.[162] DPIA를 규정하고 있는 GDPR 제35조는 이러한 개인정보 처리의 유형(type of processing)이 특히 새로운 기술을 이용하는 경우(in particular using new technologies), 해당 처리의 위험성을 반드시 고려하여야한다고 규정하고 있는 바, 이러한 새로운 기술에는 빅 데이터 분석을 포함한 프로파일링 기법이 포함되어 있다 할 것이다.

특히, DPIA가 반드시 요구되는 경우를 다루고 있는 동 조항 3항(a)은 프로파일링 등의 자동화 처리에 근거하여, 정보주체의 개인적 측면에 관한 체계적이고 광범위한 평가가 이루어지고, 그러한 평가에 근거한 결정이 해당 개인에게 법적 효력을 미치거나 이와 유사하게 중대한 영향을 미치는 경우를 명시적으로 규정하고 있는 바,[163] 모든 빅 데이터 분석은 -해당 분석에 활용되는 정보가 가명처리정보를 포함한 개인정보에 해당하는 한 -반드시 DPIA의 평가 대상이 된다 할 것이다. 다시 말해, 빅 데이터 분석을 포함하여 정보주체의 개인적 측면을 분석하기 위한 프로파일링은 해당 개인정보를 처리하기 이전에 반드시 그 위험성을 평가받아야 하는 것이다.

특히 1995년 개인정보보호지침에는 존재하지 않았던 DPIA 제도의 취지를 설명하고 있는 해설전문 89항은 DPIA가 프로파일링 등 새로운 개인정보 처리 기술에 따라 정보주체의 권리가 침해되는 것을 최소화하기 위하여 도입

162) GDPR Art. 35. 1.

163) GDPR Art. 35. 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.

되었다는 사실을 명시하고 있다.[164] 즉, 과거 모든 개인정보의 처리를 감독당국에게 일일이 통보해야만 했던 지침의 규정은 행정적·재정적 부담만을 초래할 뿐, 개인정보보호를 강화하는데 아무런 기여를 하지 못하였으므로, GDPR에서는 특별히 위험성이 높다고 예견되는 유형의 개인정보 처리에 한하여 DPIA를 실시한다는 것인데, 새로운 기술을 이용한 프로파일링은 이러한 유형에 포함되는 것이다.

## 1.2. 프로파일링과 관련된 정보주체의 권리

### 1.2.1. 정보를 제공받을 권리

GDPR에서 규정하는 투명성 원칙에 따라 개인정보처리자는 정보주체로 하여금 자신의 개인정보 처리와 관련된 세부 사항을 알 수 있도록 보장하여야 하며, 이러한 사항에는 개인정보의 프로파일링 처리 여부와 프로파일링에 대한 결과가 포함된다.[165] 앞서 언급한 바와 같이, GDPR은 정보주체가 가지는 정보를 제공받을 권리(right of information)를 개인정보가 정보주체로부터 수집된 경우(제13조)와 정보주체 이외로부터 수집된 경우(제14조)로 구분하고 있는데, 프로파일링에 대한 고지 여부는 각각의 경우에 따라 다르게 규정되고 있다.

먼저, 개인정보가 정보주체로부터 직접 수집되는 경우, 개인정보처리자는 프로파일링을 포함한 자동화된 방식에 따른 의사결정(automated

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

165) GDPR Recital (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.

decision-making)의 존재 여부, 이러한 처리방식에 수반된 논리구조에 관한 유의미한 정보, 그리고 정보주체에게 있어서 해당 처리의 중요성 및 예상되는 결과를 정보주체에게 고지하여야 한다.[166] 해당 정보를 정보주체가 이미 인지하고 있는 경우를 제외하고, 이러한 고지의무의 이행에는 어떠한 예외사유도 존재하지 않는다.[167]

> *Article 13 Information to be provided where personal data are collected from the data subject*
>
> 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:
> (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.

개인정보가 정보주체 이외로부터 수집된 경우에도, 개인정보처리자는 프로파일링과 관련된 상기 정보를 정보주체에게 고지하여야 한다.[168] 다만, 정보주체 이외로부터 수집한 개인정보에 대한 고지의무는 동 규정 제89조 1항에 따라 가명처리 등 안전조치를 확보한'공익을 위한 기록보존, 과학 및 역사연구, 통계적 목적'에 따른 개인정보 처리에 있어서 개인정보처리자로 하여금 불균형적인 노력을 요하는 경우 요구되지 않는다.[169]

---

166) GDPR Art. 13. 2(f).
167) GDPR Art. 13. 3.
168) GDPR Art. 14. 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: (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.
169) GDPR Art. 14. 5. Paragraphs 1 to 4 shall not apply where and insofar as: ... (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;

### 1.2.2. 프로파일링 정보에 대한 접근권

GDPR에 규정된 접근권(right of access)에 따라 정보주체는 프로파일링과 관련한 일련의 정보를 취득할 권리를 가진다(제15조 1항 (h)).[170] 이때 정보주체가 접근할 수 있는 정보라 함은, 프로파일링을 포함한 자동화된 방식에 따른 의사결정(automated decision-making)의 존재 여부, 이러한 처리방식에 수반된 논리구조에 관한 유의미한 정보, 그리고 정보주체에게 있어서 해당 처리의 중요성 및 예상되는 결과로서 상기 제13조 내지 제14조의 문언과 동일하다.

### 1.2.3. 반대권 및 자동화된 개별 의사결정

특히 프로파일링과 관련하여 정보주체의 권리를 강조하고 있는 규정은 처리를 반대할 수 있는 권리를 다룬 제21조와 프로파일링을 포함한 자동처리방식에 따른 의사결정에 종속되지 않을 권리를 다룬 제22조이다. 정보주체의 권리를 규정한 GDPR 제3장 가운데 제4부 'Right to object and automated individual decision-making'을 구성하고 있는 두 조항을 살펴보면 다음과 같다.

먼저, 정보주체로 하여금 자신의 개인정보 처리를 반대할 수 있는 권리(right to object)를 규정한 제21조는 크게 세 가지 경우를 구분하고 있다. 첫째, 직접 마케팅(direct marketing)을 목적으로 자신의 개인정보가 처리되는 경우, 정보주체는 언제든지 이에 대하여 반대할 권리를 가지며, 그러한 마케팅에 프로파일링이 연관된다면, 해당 프로파일링은 더 이상 직접 마케팅을 목적으로 처리될 수 없다.[171]

| *Article 21 Right to object* |
| --- |
| 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 |

170) Article 15 Right of access by the data subject
1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and where that is the case, access to the personal data and the following information: (h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

171) GDPR Art. 21 3.

data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.
3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

둘째, 프로파일링을 포함한 개인정보의 처리가 1)공익상의 이유 또는 개인정보처리자에게 부여된 공적권한의 행사를 위하여 필요한 경우 또는 2)개인정보처리자가 추구하는 정당한 이익을 추구하기 위하여 필요한 경우라 하더라도, 정보주체는 언제든지 그러한 처리에 반대할 권리를 가진다. 이때, 개인정보처리자는 개인정보의 처리가 1)정보주체의 이익, 권리 및 자유에 우선한다는 사실, 또는 2)청구권의 입증, 행사 또는 방어(establishment, exercise or defence of legal claims)에 필요하다는 사실을 입증하지 못할 경우, 해당 개인정보를 처리할 수 없다.[172]

셋째, 제89조 1항에 따른 과학·역사연구 목적 또는 통계 목적으로 개인정보가 처리되는 경우, 정보주체의 반대권은 해당 처리가 공익상 이유로 이행되는 업무의 수행을 위해 필요한 경우를 제외하고 인정된다.[173]

Article 21 Right to object

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.

이상을 살펴보면, 개인정보처리자가 시장조사와 같은 직접 마케팅을 목적으로 개인정보를 빅 데이터 분석에 활용하는 경우, 정보주체는 해당 처리를 언제든지 반대할 수 있다. 이와 달리, 가명처리를 포함한 안전조치가 확보된 상황에서 공익에 따른 과학·역사 연구 또는 통계 목적에 따른 프로파일링에

172) GDPR Art. 21 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.
173) GDPR Art. 21 6.

대하여 정보주체는 반대권을 행사할 수 없다. 다시 말해, 통계 목적에 따른 개인정보의 처리에는 시장조사를 목적으로 하는 빅 데이터 분석이 포함될 수 있지만, 이러한 상업용 통계 목적에 따른 개인정보의 프로파일링이 제5조, 제6조, 및 제89조에 따른 목적 외 처리로서 무조건적으로 허용되는 것은 아니라는 것이다.

다음으로, 정보주체는 프로파일링을 포함하여 오로지 자동화된 방식에 의한 개인정보 처리에 따른 의사결정이 자신에 대한 법적 효력을 초래하거나 이에 상응하는 정도로 중대한 영향을 미치는 경우, 그러한 의사결정에 구속되지 않을 권리를 가진다(제22조 1항). 즉, GDPR은 프로파일링을 통한 개인정보의 활용을 허용하는 한편, 사람의 개입이 전혀 이루어지지 않은 상황에서, 프로파일링과 같은 자동화된 방식에 의한 개인정보 처리에 근거하여 정보주체에 대한 평가가 이루어지는 상황을 경계하고 있는 것이다.

이처럼 GDPR은 공익을 위한 기록보존, 과학 및 역사 연구, 통계적 목적에 따른 목적 외 처리를 허용하는 한편, 빅 데이터 분석과 같은 프로파일링과 자동화된 방식에 의한 개인정보 처리에 대한 관련 규정을 별도로 규율함으로써, 개인정보의 활용과 정보주체의 권리 사이에 균형을 모색하고 있다.

### 1.3. 개인정보보호법

이와 달리, 개인정보보호법은 빅 데이터 분석과 같은 프로파일링에 해당하는 개인정보 처리의 유형을 별도로 정의하고 있지 않다. 법률에 프로파일링에 대한 정의가 없으므로, 해당 처리에 대한 관련 규정 역시 존재할 수가 없다. 예를 들어, GDPR은 프로파일링을 통한 개인정보 처리를 DPIA의 평가 대상으로 명시적으로 규정하고 있지만, 개인정보보호법에 따른 영향평가의 대상은 산술적 기준에 근거하여 산정될 뿐, 해당 개인정보파일의 처리가 프로파일링 기법을 사용하고 있는지 여부를 따지지 않는다. 또한, 개인정보 처리 사항을 정보주체에게 고지하도록 규정한 GDPR 제13조는, 개인정보 수집에 따른 고지의무를 규정하고 있는 개인정보보호법 제15조와 비교되는데, 전자가 프로파일링과 관련한 일련의 사항 -프로파일링 존재 여부, 수반된 논리 구조에 관한 유의미한 정보, 정보주체에게 있어서 프로파일링 처리의 중요성 및 예상되는 결과 -을 고지내용으로 규정하는 것과 달리, 후자는 이러한 정

보를 고지내용으로 포함시키지 않고 있다.

### 1.4. 개인정보보호법제 개선방향

GDPR의 프로파일링 규정을 참조하여 법률에 프로파일링에 대한 별도의 개념을 규정할 필요가 있으며, 개인정보처리자가 프로파일링 시 프로파일링의 존재여부, 수반된 논리구조에 관한 유의미한 정보, 프로파일링 처리의 중요성 및 예상되는 결과 등을 정보주체에게 고지하도록 규정할 필요가 있다. 또한 정보주체가 프로파일링을 포함하여 오로지 자동화된 방식에 의한 개인정보 처리에 따른 의사결정이 자신에 대한 법적 효력을 초래하거나 이에 상응하는 정도로 중대한 영향을 미치는 경우, 그러한 의사결정에 구속되지 않을 권리를 명시하는 방향으로 개인정보보호법을 개선한 필요가 있다.

## 2. 동의

### 2.1. 동의의 개념

정보주체가 하나 이상의 구체적 목적에 관하여 자신의 개인정보 처리에 대하여 동의(consent)를 주었으면 그 처리는 적법하다.[174] 동의는 개인정보처리자 등의 정당한 이익, 계약의 집행 등을 위하여 필요한 경우와 함께 개인정보의 적법한 처리의 법적 근거가 된다.[175] 동의는 동일한 목적(들)을 위하여 수행된 모든 처리행위를 다룬다.[176] 처리가 다중의 목적을 가진 경우, 동의는 이들 목적 모두에 대하여 주어져야 한다.[177] 정보주체의 동의가 전자적 수단에 의한 요청에 따라 주어진다면, 동 요청은 분명하고, 간결하며 제공되는 서비스의 이용에 불필요하게 지장을 주지 말아야 한다.[178]

---

174) GDPR 제6(1)(a).

175) 1995년 개인정보보호지침에 따라 정보주체가 준 동의에 근거하여 개인정보를 수집하여 처리하고 있는 경우 개인정보처리자는 동 동의가 주어진 방식이 GDPR의 조건에 일치한다면 새로이 동 정보주체의 동의를 얻을 필요는 없다. GDPR Recital 제171항. 1995년 개인정보보호지침에 따라 채택된 유럽위원회 결정과 감독당국의 허가도 GDPR에 따라 개정되고, 대체되거나 폐기될 때까지 계속 유효하다. Id. 따라서, 개인정보처리자가 GDPR에 규정된 동의의 높은 기준을 충족할 수 없는 경우에 개인정보 처리의 다른 법적 근거를 찾거나 더 이상 해당 개인정보 처리를 할 수 없게 된다. Information Commissioner's Office (UK), *Overview of the General Data Protection Regulation (GDPR)* 9 (July 2016).

176) GDPR Recital 제32항.

177) GDPR Recital 제32항.

178) GDPR Recital 제32항.

GDPR에서 동의는 '정보주체가 진술로 또는 분명한 긍정하는 행위로 자신에 관련되는 개인정보의 처리에 대한 합의를 나타내는 자신의 의도의 자유롭게 주어지고, 구체적이며, 고지에 입각하고 모호하지 않은 표시 (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)'라고 정의된다.[179]

[표 4-1] 1995년 개인정보보호지침으로부터 2016년 GDPR 채택까지 동의 개념의 변화

| 1995 Directive | European Commission Proposal (25 Jan. 2012); Draft European Parliament Legislative Resolution (21 Nov. 2013) | Opinion of the Committee on Industry, Research and Energy (26 Feb. 2013) | Consolidated text of the Commission and Council (informal after 31 Dec. 2014); Compromise Text of the Council (11 June 2015) | 2016 GDPR |
|---|---|---|---|---|
| | | | | |
| 'consent': any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed. | (8) 'the data subject's consent' means any freely given specific, informed and **explicit** indication of his or her wishes by which the data subject, **either by a statement or by a clear affirmative action**, signifies agreement to personal data relating to them being processed | (8) 'the data subject's consent' means any freely given specific, informed and **u n a m b i g u o u s** indication of his or her wishes by which the data subject signifies agreement to personal data relating to them being processed. Silence or inactivity does not in itself indicate consent | (8) 'the data subject's consent' means any freely-given,specific and informed ~~e x p l i c i t / ( … )~~ indication of his or her wishes bywhich the data subject, **either by a statement or by a clear affirmative action,** signifies agreement to personal data relating to them being processed; | 'consent': any freely given, specific, informed and **u n a m b i g u o u s** indication of his or her wishes by which the data subject, either b**y a statement or by a clear affirmative action**, signifies agreement to personal data relating to him or her being processed. |

동의의 정의에 관하여 GDPR은 1995년 개인정보보호지침과 기본적으로 동일한 구조를 갖지만, 다음의 두 가지 조건을 추가하였다. 첫째, GDPR은 개인정보 처리에 대한 동의가 주어지는 방식에 관하여 '자유롭게 주어지고 구체적이며 고지에 입각한 표시'에 '모호하지 않은' (unambiguous) 조건을 추가하여 '자유롭게 주어지고, 구체적이며, 고지에 입각하고 모호하지 않은 표시' (freely given, specific, informed and unambiguous indication)가 되었다.

179) GDPR 제4조 (11).

둘째, GDPR은 동의가 주어지는 방식에 관하여 '진술로 또는 분명하고 긍정하는 행위로' (by a statement or by a clear affirmative action) 조건을 추가하였다. 보통의 개인정보 처리에 대하여 유럽위원회의 초안에서와 같은 '명시적' 동의 대신에 '모호하지 않은' 동의가 되었지만, '분명하고 긍정하는 행위'의 조건이 부과됨으로써 GDPR에서 보통의 개인정보 처리에 대한 동의의 수준이 높아졌다고 볼 수 있다.

[표 4-2] 1995년 개인정보보호지침과 GDPR의 동의의 정의

| 1995년 개인정보보호지침 제2(h)조 | 2016 GDPR 제4조(11). |
|---|---|
| 정보주체가 자신에 관련되는 개인정보가 처리되고 있음에 대한 합의를 나타내는 자신의 의도의 자유롭게 주어지고 구체적이며 고지에 입각한 표시 | 정보주체가 **진술로 또는 분명하고 긍정하는 행위로** 자신에 관련되는 개인정보의 처리에 대한 합의를 나타내는 자신의 의도의 자유롭게 주어지고, 구체적이며, 고지에 입각하고 **모호하지 않은** 표시 |
| any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed | 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 |

### 2.1.1. 진술로 또는 분명하고 긍정하는 행위

GDPR은 동의를 정보주체가 '진술로 또는 분명하고 긍정하는 행위로' 자신에 관련되는 개인정보의 처리에 대한 합의를 나타내는 자신의 의도의 '자유롭게 주어지고, 구체적이며, 고지에 입각하고 모호하지 않은 표시'라고 정의한다.[180] 여기서 '분명하고 긍정하는 행위'는 '자유롭게 주어지고, 구체적이며, 고지에 입각하고 모호하지 않는 표시'를 확정하는 것이다.[181] 또한, '진술'은 '분명하고 긍정하는 행위'의 한 예가 될 것인데, 전자적 수단에 의한 것을 포

180) GDPR 제4조 (11).
181) GDPR Recital 제32항.

함하는 서면의 진술은 물론 구두의 진술도 해당한다.[182] '분명하고 긍정하는 행위'는 인터넷 웹사이트를 방문할 때 박스에 체크 표시를 하거나, 정보사회 서비스를 위한 기술적 세팅을 선택하거나, 정보주체가 자신의 개인정보의 제안된 처리를 수락함을 분명하게 표시하는 '다른 진술 또는 행동' (another statement or conduct)을 포함할 수 있다.[183] 따라서, 침묵, 이미 체크 표시된 박스 (pre-ticked boxes) 또는 부작위 (inactivity)는 동의가 되지 않는다.[184]

### 2.1.2. 동의의 네 가지 표시 요소

동의는 자유롭게 주어지고, 구체적이며, 고지에 입각하고 모호하지 않은 표시라는 네 가지 요소를 가진다. 첫째, 정보주체의 동의는 자유로이 주어져야 한다. 이러한 요건은 동의를 철회하는 것이 동의를 주는 것처럼 쉬워야 한다는 동의의 조건에서도 확인된다.[185] 정보주체와 개인정보처리자 사이에서, 특히 개인정보처리자가 공공당국인 경우, '분명한 불균형' (a clear imbalance)이 있다면, 동의는 자유롭게 주어지지 않은 것으로 추정되고 그 동의는 개인정보 처리를 위하여 법적으로 유효한 근거가 되지 않는다.[186] 또한, 개별적 경우에 적절함에도 불구하고 다른 개인정보 처리 작업에 별개의 동의가 주어지게 허용되지 않으면, 또는 서비스 제공을 포함하는 계약의 이행이 동 이행에 필요하지 않은 동의에 의존한다면, 그 동의는 자유롭게 주어진 것으로 추정되지 않는다.[187] 따라서, 개인정보처리자는 자신이 제공하는 서비스를 위하여 필요하지 않는 개인정보 처리에 대한 동의를 조건으로 할 수는 없다.

둘째, 동의는 구체적이어야 한다. 따라서, 어떤 구체적 목적을 위한 개인정보 처리에 대한 동의는 다른 목적의 처리에 대한 동의와 구별되어야 한다. 예컨대, 온라인 구매 상품의 배달을 위한 개인정보 처리에 대한 동의는 마케팅 목적으로 제3자와의 개인정보 공유에 동의하는 것과 구별되어야 한다. 동의가 각각의 개인정보 처리 작업에 구체적이어야 하는 점에서, 정보주체의 동의가 다른 사안들에도 관련되는 '서면의 선언' (written declaration)의 문맥에서 주어진다면, 동 동의의 요청은 '분명하고 평범한 언어' (clear and plain

182) GDPR Recital 제32항.
183) GDPR Recital 제32항.
184) GDPR Recital 제32항.
185) GDPR 제7(3)조 제4문 참조. shall이 사용되어 법적으로 강제적이다.
186) GDPR Recital 제43항 제1문.
187) GDPR 제7(4)조 및 Recital 제43항 제2문.

language)를 사용하여 '알기 쉽고 쉽게 접근할 수 있는 형식으로' (in an intelligible and easily accessible form) 다른 사안들과 분명하게 구별되는 방식으로 제시되어야 한다.[188] 이러한 동의 선언은 부당한 조건을 포함하지 말아야 한다.[189]

셋째, 동의는 고지에 입각하여야 한다. 즉, 동의를 주기 전에 정보주체는 동의를 주는 것을 고지받아야 한다.[190] 또한, 정보주체는 동의를 주기 전에 최소한 개인정보처리자는 물론 자신의 개인정보를 처리하려는 의도된 목적을 알아야 할 것이다.[191] 정보주체는 개인정보 처리의 모든 다른 목적도 알아야 할 것이다. 또한, 정보주체는 개인정보 처리에 대한 동의를 철회할 권리나 프로파일링을 포함한 자동화된 의사결정의 존재를 고지받아야 한다.[192] 특히 '다른 사안에 관한 서면 선언' (a written declaration on another matter)의 맥락에서 정보주체가 동의가 주어지는 사실과 그 한도를 알도록 보장되어야 한다.[193]

넷째, 동의는 모호하지 않아야 한다. 1995년 개인정보보호지침은 개인정보의 정당한(legitimate) 처리의 첫 번째 기준으로서 정보주체가 '모호하지 않게' (unambiguously) 동의할 것을 요구한다.[194] 1995년 개인정보보호지침과 달리 GDPR은 개인정보 처리의 적법성 (lawfulness)의 첫 번째 기준으로서 정보주체가 하나 이상의 구체적 목적에 관하여 자신의 개인정보 처리에 대하여 동의를 준 것을 요구하지만, 동의를 줌에 '모호하지 않게' 할 것을 명시적으로 요구하지 않는다.[195] 그럼에도, GDPR은 동의의 정의에서 기본적으로 '모호하지 않은' (unambiguous) 동의를 요구하기 때문에 정당성 내지 적법성의 기준으로서 '모호하지 않은' 동의의 요구는 사실상 동일하다고 볼 수 있다.[196]

---

188) GDPR 제7(2)조 제1문. shall이 사용되어 법적으로 강제적이다. 이 경우 개인정보처리자가 미리 작성한 동의 선언 (a declaration of consent)에 대하여 EU이사회지침 93/13/EEC (Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (OJ L 95, 21.4.1993, p. 29))이 적용된다. GDPR Recital 제42항.
189) GDPR Recital 제42항.
190) GDPR 제7(3)조 제3문. shall이 사용되어 법적으로 강제적이다.
191) GDPR Recital 제42항.
192) 각각 GDPR 제13(2)(c)조 및 제14(2)(g)조.
193) GDPR Recital 제42항.
194) 1995년 개인정보보호지침 제7(a)조.
195) GDPR 제6(1)(a)조.
196) GDPR 제4조(11).

[표 4-3] 1995년 개인정보보호지침의 정당성과 GDPR의 적법성 요건으로서 동의

| Section II CRITERIA FOR MAKING DATA PROCESSING LEGITIMATE, Art.7 | **CHAPTER II PRINCIPLES** *Article 6 Lawfulness of processing* |
|---|---|
| (a) 정보주체는 **모호하지 않게** 자신의 동의를 주었다 | 1(a) 정보주체는 하나 이상의 구체적 목적에 관하여 자신의 개인정보 처리에 대하여 동의를 주었다 |
| (a) the data subject has **unambiguously** given his consent | 1(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes |

유럽위원회는 2012년에 제안한 GDPR 초안에서 모든 경우 즉 보통의 개인정보와 민감정보 처리에 명시적 동의를 요구하였다. 유럽위원회는 명시적 기준이 모호하지 않은 동의와의 '혼란스런 유사성' (confusing parallelism)을 피하기 위하여 그리고 동의의 하나의 일관된 정의를 가지기 위하여, 따라서 정보주체가 '자신이 동의를 주는지 및 무엇에 주는지' (that, and to what, he or she gives consent)의 인식을 보장하도록 추가되었다고 밝혔다.[197] 그러나 동의의 개념은 2015년 12월 유럽위원회, EU이사회 및 유럽의회의 삼자협상에서 타결되었는데, 보통의 개인정보 처리에 대하여 모호하지 않은 동의가 되었고, 민감정보에 대하여 명시적 동의가 되었다.

이러한 타협에 따라 보통의 개인정보의 처리에 대한 모호하지 않은 동의 및 민감정보의 처리에 대한 명시적 동의의 요구는 모호하지 않은 동의와 명시적 동의의 차이가 존재하는 것으로 보게 한다. 민감정보 처리에 요구되는 명시적 동의는 보통의 개인정보 처리에 요구되는 모호하지 않은 동의 보다 더 높은 수준의 동의일 것이다. 다만, 유럽위원회 초안에서 제시된 '분명하고 긍정하는 행위'로 동의가 주어져야 한다는 조건은 최종적으로 반영되어서, '모호하지 않은' 동의의 기준이 보다 강화된 것으로 볼 수 있을 것이다.

## 2.2. 동의의 조건

197) European Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25.1.2012, COM(2012) 11 final p. 8.

GDPR은 동의의 조건을 다음과 같이 규정한다. 첫째, 개인정보 처리가 동의에 근거할 때, 개인정보처리자는 정보주체가 자신의 개인정보 처리에 동의하였음을 입증할 수 있어야 한다.[198] 따라서 개인정보처리자는 언제 및 어떻게 동의가 주어졌는지의 기록을 보관하여야 할 것이다.[199] 이렇게 동의의 입증책임과 의무는 동의가 '자유롭게 주어지고, 구체적이며, 고지에 입각하고 모호하지 않은 표시'라는 요건을 충족시키는 것을 확인하게 하면서, 또한 개인정보처리자의 개인정보 처리의 다양한 목적에 따른 동의의 존재를 확인할 수 있도록 준비하게 할 것이다.

둘째, 정보주체의 동의가 다른 사안들에도 관련되는 '서면의 선언' (written declaration)의 문맥에서 주어진다면, 동의의 요청은 '분명하고 평범한 언어' (clear and plain language)를 사용하여 '알기 쉽고 쉽게 접근할 수 있는 형식으로' (in an intelligible and easily accessible form) 다른 사안들과 분명하게 구별되는 방식으로 제시되어야 한다.[200] 본 규칙의 위반이 되는 이러한 선언의 어느 부분도 법적으로 구속력이 있지 않다.[201]

셋째, 정보주체는 자신의 동의를 언제라도 철회할 권리를 가져야 한다.[202] 동의의 철회는 그 철회 전에 동의에 근거한 처리의 적법성에 영향을 주지 않아야 한다.[203] 동의를 주기 전에 정보주체는 동의를 주는 것을 고지받아야 한다.[204] 특히 개인정보처리자는 개인정보를 수집할 때 정보주체에게 '공정하고 투명한 처리' (fair and transparent processing)를 보장하는데 필요한 정보를 제공하여야 하는데, 이러한 정보에는 개인정보 처리의 법적 근거가 정보주체의 동의인 경우 언제라도 동의를 철회할 권리의 존재가 포함된다.[205] 동의를 철회하는 것은 동의를 주는 것처럼 쉬워야 한다.[206] 따라서, 동의가 체크 표시와 같은 행위를 통하여 주어진 경우 그 동의는 이와 유사하게 간

198) GDPR 제7(1)조. shall이 사용되어 법적으로 강제적이다.
199) 개인정보처리자 및 적용 가능한 경우 그의 대표는 자신의 책임 아래의 개인정보 처리의 기록을 유지하여야 하는데, 동 기록에 수록되는 정보에는 정보주체의 동의에 관련되는 정보는 포함되지 않는다. GDPR 제30(1)조.
200) GDPR 제7(2)조 제1문. shall이 사용되어 법적으로 강제적이다.
201) GDPR 제7(2)조 제2문. shall이 사용되어 법적으로 강제적이다.
202) GDPR 제7(3)조 제1문. shall이 사용되어 법적으로 강제적이다.
203) GDPR 제7(3)조 제2문. shall이 사용되어 법적으로 강제적이다.
204) GDPR 제7(3)조 제3문. shall이 사용되어 법적으로 강제적이다.
205) GDPR 제13(2)(c)조. 이 경우 동의가 철회되어도 철회 전에 그 동의에 근거한 처리의 적법성은 영향을 받지 않는다. Id.
206) GDPR 제7(3)조 제4문. shall이 사용되어 법적으로 강제적이다.

단하고 용이하게 접근할 수 있는 행위를 통하여 철회되어야 한다. 일단 동의가 철회되면, 정보주체는 자신의 개인정보가 삭제되고 더 이상 처리를 위하여 이용되지 않게 할 권리를 가진다.

넷째, 동의가 자유로이 주어지는지를 평가할 때, 서비스 제공을 포함하여 계약의 이행 등이 동 계약의 이행에 필요하지 않은 개인정보의 처리에 대한 동의를 조건으로 하는지가 최대한 고려되어야 한다.[207]

## 2.3. 아동의 동의

GDPR은 아동의 구체적 보호를 위하여 그 부모의 허락 없이 개인정보 처리에 대한 동의를 하는 능력을 제한한다. 아동은 자신의 개인정보 처리에 관련하여 위험, 결과 및 해당 안전조치 및 권리를 이해하기 어려울 수 있기 때문이다.[208] 특히 정보사회서비스 (information society services)의 제공에 필요한 아동의 개인정보 수집, 마케팅 또는 신원 (personality) 또는 이용자 프로파일의 창출에 있어 아동의 보호가 필요하기 때문이다.[209] 이러한 동의 능력의 제한은 Facebook과 같은 SNS를 의미하는 정보사회서비스의 이용에 관련하여 의미를 갖는다.

첫째, 정보주체의 동의가 자신의 개인정보의 적법한 처리의 법적 근거가 될 때, 아동에 대한 직접적인 정보사회서비스의 제공에 관련하여, 아동의 개인정보 처리는 아동이 적어도 16살이 될 때 적법하다.[210] 아동이 16살 미만일

---

207) GDPR 제7(4)조. shall이 사용되어 법적으로 강제적이다.

208) GDPR Recital 제38항.

209) GDPR Recital 제38항. 정보사회서비스는 '전자적 수단으로 및 서비스 수령자의 개별적 요청으로 원거리에서 수익을 목적으로 통상적으로 제공되는 서비스'를 의미한다. GDPR 제4조 (25) 및 Directive (EU) 2015/1535 of the European Parliament and of the Council1 제1(1)(b)조.

210) GDPR 제8(1)조 제1문. shall이 사용되어 법적으로 강제적이다. 아동에게 직접 제공되는 서비스의 이용을 위하여 아동에 관한 개인정보가 수집되는 경우가 된다. 유럽위원회 초안은 미국의 COPPA와 같이 13살을 제안하였다. 그러나, EU이사회, 유럽의회 및 유럽위원회의 삼자협의에서 16세로 상향하도록 합의되었고, 회원국들에게 아동의 동의 최저 연령을 13세 미만이 되지 않도록 허용하였다. Gabe Maldoff, "Top 10 operational impacts of the GDPR: Part 3 - consent", iapp, The Privacy Advisor, Jan 12, 2016, https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-3-consent/. 따라서, 특정 회원국법으로 달리 규정되지 않으면, 개인정보처리자는 16세 미만 아동의 개인정보를 처리할 때 그의 부모나 후견인의 동의를 얻어야 한다. 미국의 '아동 온라인 프라이버시 보호법' (Children's Online Privacy Protection Rule: COPPA)은 1998년 채택되었는데, 13세 미만의 아동에 대한 웹사이트나 온라인서비스 조작자 및 13세 미만의 아동에게서 개인정보를 온라인으로 수집하고 있음을 실제로 알고 있는 다른 웹사이트나 온라인서비스 조작자에게 일정한 요건을 부과한다. COPPA에 관하여 https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule 참조.

때 그의 개인정보 처리는 그에 대한 친권(parental responsibility) 보유자가 동의를 주거나 허락한 경우에만 적법하다.[211] 친권 보유자의 동의는 아동에게 직접적으로 제공되는 예방적 또는 상담 서비스(preventive or counselling services)의 맥락에서는 필요하지 않다.[212] 회원국은 이러한 어린 나이가 13살 미만이 아니라면 법으로 그들 목적으로 '더 어린 나이' (a lower age)를 규정할 수 있다.[213] 이렇게 아동의 동의 최저 연령에 대한 EU회원국들 사이의 차이의 가능성으로 EU내의 여러 회원국에 걸쳐 관련 서비스를 제공하는 사업자들은 상당한 부담을 가지게 된다.

둘째, 개인정보처리자는 '이용가능한 기술' (available technology)을 고려하여 아동에 대한 친권 보유자가 동의를 주거나 허락함을 입증하도록 '합리적 노력' (reasonable efforts)을 하여야 한다.[214] 아동의 개인정보 처리에 관한 동의의 존재에 관한 개인정보처리자의 입증은 그렇게 엄격하지 않다. 그러한 입증을 위한 '합리적 노력'을 하면 되고 또한 당시 '이용가능한' 기술이 고려되기 때문이다.

셋째, 아동의 개인정보의 적법한 처리에 관한 GDPR 제8조 제1항에도 불구하고, 아동에 관련한 '계약의 효력, 성립 또는 효과' (validity, formation or effect of a contract)에 관한 규칙과 같은 회원국의 일반적 계약법은 영향을 받지 않는다.[215]

## 2.4. 기타 동의 관련 규정

이외에도 GDPR은 다음과 같이 동의에 관련된 규정을 둔다. 첫째, 정보주체는, 삭제의 권리 (right to erasure)에 따라, 자신의 동의에 근거하여 개인정보가 처리된 경우 그 동의를 철회하면 해당 개인정보처리자에게 자신의 개인정보를 삭제하라고 요구할 권리를 가진다.[216]

---

211) GDPR 제8(1)조 제2문. shall이 사용되어 법적으로 강제적이다.
212) GDPR Recital 제38항.
213) GDPR 제8(1)조 제3문. shall이 사용되어 법적으로 강제적이다. 영국은 아동의 동의 최저 연령을 13세로 정할 것이라고 보도되었다. James Titcomb, "Britain opts out of EU law setting social media age of consent at 16", The Telegraph, 16 Dec. 2015, http://www.telegraph.co.uk/technology/internet/12053858/Britain-opts-out-of-EU-law-raising-social-media-age-of-consent-to-16.html.
214) GDPR 제8(2)조. shall이 사용되어 법적으로 강제적이다.
215) GDPR 제8(3)조. shall이 사용되어 법적으로 강제적이다.

둘째, 정보주체가 개인정보 처리를 제한하는 권리를 행사하는 경우, 해당 정보주체의 동의를 얻거나 법적 권리의 확정, 행사 또는 방어를 위하여 또는 다른 자연인이나 법인의 권리 보호를 위하여 또는 EU나 회원국의 중요한 공익을 이유로, 개인정보처리자는 동 개인정보의 처리를 지속할 수 있다.[217]

셋째, 정보주체는, 개인정보 이동의 권리 (right to data portability)에 따라, 개인정보 처리가 자신의 동의에 근거하고 동 처리가 자동화된 수단으로 수행되는 경우, 개인정보처리자에게 제공한 자신에 관한 개인정보를 수령할 권리와 동 개인정보처리자로부터 동 개인정보를 다른 개인정보처리자에게 방해받지 않고 전송할 권리를 가진다.[218]

넷째, 공익을 위한 문서보관 목적, 과학 및 역사 연구 목적, 또는 통계 목적을 위한 추가적 처리는 일반적으로 원래의 수집 목적과 양립하는 것으로 간주된다.[219] 따라서 이 경우 정보주체의 동의가 요구되지 않는다. 그럼에도, 과학적 연구 목적으로 개인정보를 수집하는 경우에 동 개인정보 처리 목적을 완전하게 확인하기는 쉽지 않다. 특히 빅데이터를 활용하는 경우 더욱 그럴 것이다. 따라서 정보주체는 과학적 연구의 공인된 윤리기준에 일치하여 과학적 연구의 일정 분야에 대하여 동의를 주도록 허용되어야 한다.[220] 정보주체는 '의도된 목적이 허용한 정도까지 연구의 일정한 영역이나 연구 프로젝트의 부분에만 동의' (consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose)를 주는 기회를 가져야 한다.[221]

## 2.5. 명시적 동의가 필요한 경우

제29조 작업반에 따르면, 법적 용어로서 '명시적' (explicit) 동의는 '분명한' (express) 동의와 동일한 의미를 가진다. 명시적 동의는 '개인들에게 자신들

---

216) GDPR 제17(1)(b)조.
217) GDPR 제18(2)조.
218) GDPR 제20(1)조.
219) GDPR 제5(1)(b)조. 이 경우 정보주체의 보호를 위한 적절한 안전조치가 적용되어야 한다. GDPR 제89조 참조.
220) GDPR Recital 제33항.
221) GDPR Recital 제33항.

의 개인정보의 특정한 이용이나 공개에 대하여 동의하거나 동의하지 않는 제안이 제시되고 그들이 구두로 또는 문서로 그 문제에 대하여 적극적으로 반응하는 모든 상황' (all situations where individuals are presented with a proposal to agree or disagree to a particular use or disclosure of their personal information and they respond actively to the question, orally or in writing)을 포함한다.[222] 예컨대, 개인정보처리자가 개인정보를 수집하여 처리하고자 하는 이유를 분명하게 적시한 동의 양식에 정보주체가 서명하면 명시적 동의가 주어진 것이다.[223]

### 2.5.1. 민감정보

1995년 개인정보보호지침과 유사하게 GDPR은 건강에 관한 정보 등 '특별한 유형의 정보' (special categories of data), 즉 민감정보의 처리를 금지한다.[224] 그런데, GDPR과 1995년 개인정보보호지침은 정보주체가 이러한 개인정보의 처리에 대하여 '명시적' (explicit) 동의를 주는 경우에 이러한 금지에 대한 예외를 인정한다.[225] 따라서 GDPR과 1995년 개인정보보호지침은 민감정보의 처리에 대하여 정보주체의 명시적 동의를 요구하는 점에서 동일하다. 1995년 개인정보보호지침과 유사하게, GDPR은 EU법 또는 회원국법이 정보주체의 명시적 동의에 의하여 이들 민감정보의 처리 금지가 해제되지 않을 수 있게 규정한다.[226]

한편, 1995년 개인정보보호지침과 비교하여 GDPR은 이러한 민감정보의 범위를 상당하게 확대하여 명시적 동의가 요구되는 경우가 확대되어 이러한 개인정보의 처리는 보다 더 엄격하게 된 것으로 볼 수 있다. 즉, GDPR은 유전데이터, 자연인을 고유하게 식별하는 목적의 생체데이터, 자연인의 성적 성향에 관한 데이터를 민감정보에 추가하였다.[227] 참고로 사진은 '자연인의

222) Opinion 15/2011 on the definition of consent, adopted on 13 July 2011, WP187, p. 25.
223) Opinion 15/2011 on the definition of consent, adopted on 13 July 2011, WP187, p. 25.
224) 1995년 개인정보보호지침 제8(1)조 및 GDPR 제9(1)조.
225) 1995년 개인정보보호지침 제8(2)(a)조 및 GDPR 제9(2)(a)조.
226) 1995년 개인정보보호지침 제8(2)(a)조 단서 및 GDPR 제9(2)(a)조 단서. 1995년 개인정보보호지침은 회원국법만 언급한다.
227) 유전데이터 (genetic data)는 '자연인의 자연인의 생리 또는 건강에 관한 고유한 정보를 주고 특히 해당 자연인의 생물학적 샘플의 분석에서 결과하는 유전되거나 획득한 유전적 특성에 관련된 개인정보'라고 정의된다. GDPR 제4조 (13). 생체데이터 (biometric data)는 '자연인의 신체적, 생리

고유한 식별 또는 증명을 허용하는 구체적 기술적 수단' (a specific technical means allowing the unique identification or authentication of a natural person)을 통하여  처리될 때에만 생체데이터가 된다.[228]

[표 4-4] 1995년 개인정보보호지침과 GDPR의 민감정보

| Article 8<br>특별한 유형의 개인정보 처리 (The processing of special categories of data) | Article 9 특별한 유형의 개인정보 처리 (Processing of special categories of personal data) |
|---|---|
| 1. 회원국들은 인종적 또는 민족적 출신, 정치적 의견, 종교적 또는 철학적 믿음, 노조 가입을 드러내는 개인정보의 처리, 및 건강 또는 성생활에 관한 데이터의 처리를 금지해야 한다 | 인종적 또는 민족적 출신, 정치적 의견, 종교적 또는 철학적 믿음, 또는 노조 가입을 드러내는 개인정보의 처리, 및 **유전데이터, 자연인을 고유하게 식별하는 목적의 생체데이터**, 건강에 관한 데이터 또는 자연인의 성생활 또는 **성적 성향에 관한 데이터**의 처리는 금지되어야 한다 |
| 1 . Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life | 1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of **genetic data, biometric data for the purpose of uniquely identifying a natural person**, data concerning health or **data concerning** a natural person's sex life or **sexual orientation** shall be prohibited |
| 2(a) 정보주체는 그들 데이터의 처리에 자신의 **명시적** 동의를 주었다 | 2(a) 정보주체는 하나 이상의 구체화된 목적에 관하여 그들 개인정보의 처리에 |

적, 또는 행태적 특성에 관련된 구체적 기술적 처리에서 결과하고, 안면 이미지나 지문검사 데이터와 같은 그 자연인의 고유한 식별을 허용하거나 확정하는 개인정보'라고 정의된다. GDPR 제4조 (14).

228) GDPR Recital 제51항.

| | |
|---|---|
| | **명시적** 동의를 주었다 |
| 2(a) the data subject has given his **explicit** consent to the processing of those data ... | 2(a) the data subject has given **explicit** consent to the processing of those personal data for one or more specified purposes ... |

### 2.5.2. 자동화된 의사결정

정보주체는 자신에 관한 법적 효과를 주거나 자신에게 유사하게 상당하게 영향을 주는 프로파일링을 포함하여 자동화된 처리에만 근거한 결정에 따르지 않을 권리를 가져야 한다.[229] 그러나, 이러한 결정이 정보주체의 '명시적 동의' (explicit consent)에 근거하면, 동 결정에 따를 수 있다.[230] 따라서 일반적 이용 조건에 대한 이용자의 수동적 묵인은 유효한 동의가 되지 않는다.

### 2.5.3. 제3국에 대한 이전

1995년 개인정보보호지침과 유사하게 GDPR은 개인정보의 제3국으로의 이전에 동 제3국이 '적정한 보호 수준' (adequate level of protection)을 보장하도록 요구한다.[231] 그런데, GDPR 제45(3)조에 따른 적정성 결정 또는 구속력 있는 기업규칙 (BCRs)을 포함한 제46조에 따른 적절한 안전조치가 없는 경우, 이러한 적정성 결정과 적절한 안전조치의 결여에 따른 정보주체에 대한 가능한 위험을 고지받은 후에, 정보주체가 자신의 개인정보의 제3국 또는 국제기구에 대한 제안된 이전에 대하여 '명시적으로 동의한' (has explicitly consented) 경우에 동 이전이 가능하다.[232]

한편, 1995년 개인정보보호지침은 정보주체가 동 제안된 이전에 대하여 '모호하지 않게' (unambiguously) 자신의 동의를 주었으면 동 제안된 이전을 허용한다.[233] 따라서 GDPR은 제3국으로의 개인정보의 이전에 대하여 정보주체의 '모호하지 않은' 동의 대신 '명시적' 동의를 요구하여 동의의 기준을 높

229) GDPR 제22(1)조.
230) GDPR 제22(2)(c)조.
231) 1995년 개인정보보호지침 제25(1)조 및 GDPR 제45(1)조.
232) GDPR 제49(1)(a)조.
233) 1995년 개인정보보호지침 제26(1)(a)조.

인 것으로 볼 수 있다.

[표 4-5] 1995년 개인정보보호지침과 GDPR의 제3국 이전

| Article 26 Derogations | *Article 49 Derogations for specific situations* |
|---|---|
| 1(a) 정보주체는 제안된 이전에 **모호하지 않게** 자신의 동의를 주었다 | 1(a) 정보주체는 적정성 결정과 적절한 안전조치의 결여에 따른 정보주체에 대한 가능한 위험을 고지받은 후에, 제안된 이전에 **명시적으로** 동의하였다 |
| 1(a) the data subject has given his consent **unambiguously** to the proposed transfer | 1(a) the data subject has **explicitly** consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards |

## 2.6. 동의 규정 위반에 대한 제재

GDPR 제5조 (개인정보 처리 원칙), 6조 (처리의 적법성), 7조 (동의의 조건), 9조 (민감정보의 처리)에 따른 동의에 관한 규정의 위반에 대하여 최대 2천만유로의 과징금 (administrative fines)이 부과되거나, 기업 (undertaking)의 경우 이와 '전년도 전세계 연매출 (total worldwide annual turnover of the preceding financial year)의 최대 4% 중에서 더 높은 금액이 부과되어야 한다.[234] GDPR에 규정된 가장 과중한 처벌이 적용된다. 그러나, GDPR 제8조 (정보사회서비스에 관련된 아동의 동의에 적용되는 조건)에 따른 아동의 동의에 관한 규정의 위반에 대하여는 최대 1천만유로의 과징금 (administrative fines)이 부과되거나, 기업 (undertaking)의 경우 이와 '전년도 전세계 연매출 (total worldwide annual turnover of the preceding financial year)의 최대 2% 중에서 더 높은 금액이 부과되어야 한다.[235]

## 2.7. 소결

개인정보 처리의 법적 근거로서 정보주체의 동의는 하나 이상의 구체적 처리 목적에 대하여 '모호하지 않고' (unambiguous), 특히 민감한 개인정보에

234) GDPR 제83(5)(a)조.
235) GDPR 제83(4)(a)조.

대하여 '명시적이어야' (explicit) 하며, 정보주체는 동의를 주기 전에 철회 권리를 통지받아야 한다. 동의는 '분명하고 긍정하는 행위' (a clear affirmative action)를 통하여야 한다. 따라서 1995년 개인정보보호지침과 비교하여 GDPR에서 기업 등이 개인정보의 수집 등에 관하여 정보주체의 동의를 얻는 것은 보다 어렵게 된다. 그러나, 기업 등에게 다행스러울 점은 명시적인 동의가 민감한 개인정보의 처리에 국한하여 요구되는 점이다.

GDPR의 기본 목적은 정보주체에게 자신의 개인정보에 대한 통제권을 주는 것인데, 개인정보 수집 등 처리에 있어서 정보주체의 동의의 강화가 이러한 목적에 기여할 수 있다. 그러나, 법적으로 요구되는 동의의 기준이 너무 높게 되면 개인정보 수집 등의 정당한 법적 근거로서 동의가 점차 무시될 수 있을 것이다.[236] 이러한 상황에서는 정보주체의 자신의 개인정보에 대한 통제는 GDPR에서 규정된 투명성, 이동성과 잊혀질 권리와 같은 강화된 권리를 통하여 행사될 수 있다.

GDPR의 채택 과정에서 동의는 최종적으로 EU이사회, 유럽의회 및 유럽위원회 사이에서 타협으로 결정될 정도로 뜨거운 쟁점 중의 하나였다. 비록 유럽위원회가 제안하고 유럽의회가 지지한대로 민감정보는 물론 보통의 개인정보의 수집을 포함한 처리에 명시적 동의가 요구되지 않고, 보통의 개인정보의 처리에 대하여는 모호하지 않는 동의가 요구되도록 합의되었지만, 유럽위원회가 제안한대로 모호하지 않은 동의는 '분명하고 긍정하는 행위'를 통하여 주어진다. 또한 정보주체는 동의를 주는 것과 마찬가지로 철회를 언제라도 쉽게 할 수 있게 규정되었다. 또한 정보주체와 개인정보처리자 사이에 '분명한 불균형' (a significant imbalance)이 존재하면 동의가 자유로이 주어진 것이 아니어서 그 동의는 개인정보 처리의 법적으로 유효한 근거가 되지 못한다. 이 점에서 정보주체의 동의의 요건이 강화되었다고 볼 수 있다.

# V. 결론

236) Hogan Lovells, "GDPR – A game changer for the digital economy", Chronicle of Data Protection, http://www.hldataprotection.com/2016/01/articles/international-eu-privacy/gdpr-a-game-changer-for-the-digital-economy/.

지금까지 본 연구는 개인정보보호의 바람직한 개선방향을 모색하기 위하여 GDPR의 여러 규정을 살펴보았다. 먼저, GDPR과 개인정보보호법을 전반적으로 비교한 제1장에서는 다음과 같은 결론이 도출되었다. 첫째, 개인정보보호법과 달리, GDPR은 아동에 대한 특별한 보호의 필요성을 강조하고 이를 관련 여러 조항에 명시적으로 언급하고 있다. 둘째, GDPR 제3장 제12조 내지 제22조에 따른 정보주체의 권리는 개인정보보호법에서 규정된 정보주체의 권리를 모두 포함할 뿐만 아니라, 개인정보보호법에서 다루고 있지 않는 권리를 다루고 있다. 셋째, 국내법상 영향평가는 이미 운용되고 있는 대규모 개인정보파일의 처리에 대한 위험성을 제3자인 평가기관으로 하여금 평가하도록 하는 반면, GDPR은 개인정보처리 이전에 개인정보처리자로 하여금 그러한 처리에 대한 위험성을 자체적으로 평가하도록 규정하고 있다. 평가 대상을 선정함에 있어서 산술적 기준에 근거하는 개인정보보호법과 달리, GDPR은 평가 대상이 되는 개인정보 처리의 유형을 규정하고 있으며, 평가의 결과에 따라 해당 개인정보의 처리가 위험하다고 판단되는 경우, GDPR은 사전협의 과정에서 감독당국으로 하여금 처리의 금지를 포함한 구속력있는 제재를 가할 수 있도록 규정하고 있다는 점에서 개인정보보호법의 영향평가와 차이를 보인다. 넷째, GDPR에 따른 행동강령의 제정은 개인정보보호에 관한 실무에 있어서 중요한 역할을 할 것으로 예상된다. 이는 특정 업종에 종사하는 개인정보처리자의 개인정보처리가 특정 상황에서 어떻게 규율될 수 있는지에 대한 자율적인 가이드라인 역할을 할 것으로 기대된다. 다섯째, GDPR은 국외이전에 대하여 구체적이고 세부적인 규정을 두어 유럽연합의 보호수준에 미치지 못하는 제3국 또는 국제기구로의 개인정보 이전을 금지하고 있다. 여섯째, GDPR에서 감독당국은 독립성이 보장된 국가기관으로 그 임무가 방대하고 권한이 막강하다. 또한 GDPR은 복수의 감독당국이 존재하는 경우 이에 대한 권한 배분과 협력의무를 상세하게 규정하고 있다.

다음으로 본 연구는 빅 데이터 분석 등을 포함한 개인정보의 활용을 어떠한 방식으로 촉진하고 장려시킬 것인지에 대하여 논의하였다. 국가 또는 민간기업이 활용할 수 있는 개인정보의 가치를 극대화하는 동시에, 정보주체의 권리를 보호할 수 있는 방안을 제시하기 위하여, GDPR의 목적 외 처리 규정 및 가명처리 규정을 살펴보았고, 개인정보의 비식별 처리에 관한 미국 및 일본의 개인정보보호법제에 대하여도 논의하였다. 결론적으로, 세 국가의 법제는 어떠한 경우에도 개인정보로 가역될 수 없는 완전한 익명처리를 상정

하고 있지는 않은 것으로 보인다. 그러나 이들 국가는 완전한 익명처리란 현실적으로 이루어지기 어렵다는 공통된 인식을 가지고 있으면서도, 그러한 현실을 규율하는 방식을 달리 취하였다고 볼 수 있다. GDPR은 익명처리와 가명처리를 구분하고, 재식별 가능성을 필연적으로 수반하는 가명처리정보를 개인정보로서 GDPR의 적용범위에 포섭시키는 방안을 제시하였다. 이와 달리, 미국과 일본의 개인정보보호법제는 재식별 가능성이 희박한 비식별정보 및 익명가공정보를 더 이상 개인정보로 취급하지 않는 동시에, 해당 정보가 재식별되는 것을 방지하기 위하여 재시별 금지 규정 등을 포함한 여러 관련 규정을 도입하고 있다.

빅 데이터 분석을 포함한 개인정보의 활용을 보다 폭 넓게 허용하기 위하여 GDPR을 반영하는 경우, 개인정보보호법은 가명처리정보의 목적 외 이용·제공을 허용하는 방식으로 해석·개정될 수 있다. 이와 달리, 개인정보보호법이 미국 및 일본의 법제를 반영하는 경우 - 즉, 비식별 처리된 개인정보를 더 이상 개인정보로 취급하지 않는 경우 - 학술연구 또는 통계목적 뿐만 아니라, 다른 목적에 근거한 비식별 정보의 활용 역시 허용될 수 있다.

마지막으로, 본 연구는 GDPR의 주요 쟁점으로 프로파일링과 동의 관련 규정을 개별적으로 검토하였다. 개인정보보호법과 달리, GDPR은 빅 데이터 분석과 불가분의 관계에 있는 프로파일링을 포함한 대규모 자동처리 방식에 따른 개인정보의 처리를 별도로 규율하고 있다. 이에 따라 프로파일링을 시행하는 개인정보처리자는 반드시 해당 처리의 위험성을 사전에 예측하기 위하여 개인정보 영향평가를 시행하여야만 하며, 정보주체는 인간의 개입이 전혀 존재하지 않는 자동화된 방식의 개인정보처리 결과에 종속되지 않을 권리를 가진다. 또한 동의와 관련하여, 일반적으로 정보주체의 동의는 개인정보 수집을 포함한 처리를 적법하게 만드는 기본적인 법적 근거이다. 그러나 정보주체의 동의는 개인정보 처리를 위한 다양한 법적 근거 중의 하나에 불과하며, 이러한 동의는 언제든지 철회될 수 있다는 점에서 가장 안전한 또는 안정된 법적 근거가 될 수 없다. 그럼에도 불구하고, 정보주체의 동의가 자신의 개인정보 처리를 통제하는데 가장 좋은 수단이라는 사실에는 이견이 있을 수 없다. 정보주체의 동의에 근거하여 그의 개인정보를 처리하는 개인정보처리자는 동의가 주어지는 방식과 관련 문서가 GDPR의 관련 규정에 비추어 적절한지 유의하여야 하며, 특히 동의가 주어진 사실에 대한 입증책임

이 개인정보처리자가 있음을 유의하여야 할 것이다. 동의에 근거한 개인정보의 처리가 어려운 경우, 특히 사업자인 개인정보처리자는 GDPR 제6(1)(f)에 규정된 개인정보처리자 또는 제3자의 정당한 이익에 근거한 개인정보 처리에 보다 더 큰 관심을 가질 것으로 보인다.

# <부록1> GDPR(번역문)

개인정보의 처리와 관련한 개인의 보호 및 개인정보의 자유로운 이동에 관한 유럽의회와 유럽이사회 규정 (EU) No XXX/2016
(REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data)

해설전문번역

(1) 개인정보처리의 보호는 개인의 기본적인 권리이다. 유럽연합 기본권 헌장(이하 '헌장') 제 8조 (1)항과 유럽연합기능조약(이하 TFEU)의 제 16조 (1)항에서는 모든 사람은 본인의 개인정보를 보호할 권리가 있다고 규정하고 있다.

(2) 자연인의 개인정보처리 보호, 특히 개인정보 보호,는 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) 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) 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) 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) 급격한 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 제3국 및 국제기구로의 개인정보 이전을 용이하게 하고, 개인정보를 높은 수준으로 보호해야 한다.

(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, 경제 주체 및 공공기관을 위한 법적, 실질적 확실성이 강화되어야 한다.

(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) 지침 95/46/EC에 명시된 목적과 원칙은 여전히 타당하지만, 해당 지침은 유럽 내에서 개인정보보호방침을 집행하는 데 일관성이 결여되는 문제가 있었거나, 법적으로 확실하지 않았거나, 또는 온라인으로 활동하는 개인을 보호하는데는 상당한 리스크가 있다는, 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 보호수준이 상이한 이유는 지침 95/46/EC의 집행 및 적용상의 차이가 있었기 때문이다.

(10) 일관성을 유지하고 개인을 높은 수준으로 보호하며 역내 개인정보의 이동을 막는 장애물을 제거하기 위해서, 각 국은 개인정보처리에 있어, 개인의 권리와 자유를 동일한 수준으로 보호해야한다. 개인정보 처리에 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) 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) TFEU의 제 16조 (2)항은 유럽의회와 각료이사회가 개인정보처리에 관련된 개인을 보호하는 규정과 개인정보의 자유로운 이동에 관한 규정을 정하도록 명하고 있다.

(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 일부제외시키는 조문을 포함한다. 또한 유럽연합 기관이나 기구가 이 법을 적용할 때는 중소기업의 구체적인 니즈(needs)를 고려하도록 지향하여야 한다. 중소기업의 개념은 위원회 권고 2003/361/EC에 대한 부록 제2조에 따라야 한다.

(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) 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) 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) 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.

(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) 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 엄무)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.

(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 특정기관들은 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) 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 기여한다.

(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) 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. 유럽연합 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 것ㅁ나으로는 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) 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) 회원국 법률이 국제법의 효력으로 적용되는 경우, 이 법은 회원국 내의 설립된 외교공관이나 영사관 등 유럽연합 역외 지역에 설립된 정보처리자에게도 적용될 수 있다.

(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 식별가능한지를 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 식별되었거나 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) 이 법은 망자의 개인정보에 적용되지 않는다. 회원국은 망자의 개인정보 처리에 대한 규정을 제공할 수 있다.

(28) 개인정보의 가명처리는 해당 정보주체가 갖는 위험성을 줄일 수 있으며 정보처리자와 수탁처리자가 그들의 개인정보보호의 의무를 준수할 수 있도록 돕는다. 이 법에서 명시적으로 가명처리를 도입하는 것은 여러 어떤 개인정보보호 조치를 방해할 의도가 아니다. (가명처리를 했다고 해서 정보보호 조치가 면제되는 것이 아니다.)

(29) 개인정보처리 시 가명처리의 적용에 대한 인센티브를 부여하기 위해서는, 가명처리조치는, 일반적인 분석은 허용하되, 해당 처리가 본 법을 따르고 특정 정보주체에 대한 개인정보와 연결되는 추가적인 정보가 별도로 보관되는 기술 및 관리적 조치를 취한 경우, 이러한 제반조치들이 같은 정보처리자에 의해서 자체적으로 관리될 수 있어야 한다. 개인정보를 처리하는 정보처리자는 동종의 정보처리사업체 내의 인가받은 사람을 가리킨다.

(30) 개인이 사용하는 기기(devices), 어플리케이션, 인터넷 프로토콜 주소나 쿠키정보 또는 전파식별태그 등, 기타 식별인자와 같은 툴(tool)과 프로토콜(protocol)이 제공하는 온라인 식별인자로 인해 개인이 연결될 수 있다. 특히 이러한 정보는 개인에 대한 자취를 남겨, 이러한 정보가 서버를 통해 전해지는 독특한 식별인자 및

기타 정보와 결합되는 경우, 해당 개인에 대한 프로파일을 생성하고 이들을 식별하는 데 사용될 수 있다.

(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.

(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) 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) 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) 건강관련 개인정보에는 정보주체의 과거, 현재, 혹은 미래의 신체적 또는 정신적 건강 상태의 정보를 드러내는 모든 정보주체의 건강상태에 속하는 정보가 포함

된다. 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 혹은 생체의학적 상태에 대한 정보도 포함된다.

(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 수행되는 지 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) 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.

(38) 아동은 개인정보 처리에 따른 위험성, 결과, 이에 필요한 안전장치 및 본인의 권리를 잘 인지하지 못하고 있기 때문에 본인의 개인정보와 관련하여 구체적인 보

호를 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) 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) 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.

(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 적용대상인 개인이 유럽연합재판소와 유럽인권재판소의 판례법에 따라 그 적용을 예측할 수 있어야 한다.

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

(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 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 개인

정보의 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) 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) 개인정보를 제공받는 정보처리자 등이나 제3자의 정당한 이익(legitimate interests)이 정보처리의 법적 근거와 함께 제시되어야만 하는 경우가 있다. 이 경우는, 정보주체가 정보주체와 정보처리자와의 관계를 근거로 합리적으로 예측하리라는 것을 고려해 보았을 때, 정보주체의 이익이나 자유 및 기본권이 우선되지 않는 때이다. 이러한 정당한 이익은, 정보주체가 고객이거나 정보처리자의 서비스를 이용중인 경우와 같이 정보주체와 정보처리자 간에 타당하고 적절한 관계가 있을 때, 존재할 수 있다. 어떠한 경우에든 정당한 이익의 존재에 대해서는, 정보주체가 정보수집 시점 및 정보수집 상황에서 이러한 목적으로 정보가 처리될 수 있을 것이라고 합리적으로 예상할 수 있는지 여부 등에 관한 신중한 평가가 필요하다. 정보주체의 이익과 기본권은, 특히 정보주체가 추가적인 정보처리에 대해 합리적인 예상을 하지 못한 상황에서 개인정보가 처리될 경우, 정보처리자의 이익에 우선할 수 있다. 공공기관이 개인정보를 처리하는 근거는 입법기관(the legislator)이 법으로써 규정한다는 점을 고려할 때, 공공기관이 업무를 수행하기 위하여 정보처리를 할 때에는 이러한 근거를 적용해서는 아니된다. 사기 방지의 목적에 반드시 필요한 개인정보처리 또한 해당 정보처리자의 정당한 이익에 해당한다. 직접 마케팅(direct marketing)을 목적으로하는 개인정보처리는 정당한 이익을 위해 수행된 것으로 간주될 수 있다.

(48) 사업체그룹 또는 중앙기구의 부속 기관의 일부인 정보처리자는 내부의 행정상의 목적으로 사업체그룹 내에서 개인정보를 전송하는 정당한 이익(legitimate interests)을 가질 수 있고 여기에는 고객 또는 직원의 개인정보처리가 포함된다. 사업체그룹 내에서 제3국에 소재한 사업체로의 개인정보 이전을 규정한 일반적인 원칙에는 적용되지 않는다.

(49) 네트워크와 정보보안을 담보하기 위하여 엄밀하게 필요하고 적절한 한도 내에서 행해지는 정보처리는 관련 정보주체의 정당한 이익(legitimate interests)이 된다. 네트워크 및 정보보안이란, 주어진 신뢰수준에서의 네트워크의 능력이나 정보시스템을 말하는데, 예를 들어 저장되거나(stored) 이전된(transmitted) 개인정보가 가지는 가용성(availability), 진위성(authenticity), 무결성(integrity) 및 기밀성(confidentiality)을 위협하게 되는 돌발적 사고나 불법·악의적인 행동을 견딜 수 있는 네트워크 능력이나 정보시스템을 의미한다. 또 다른 예로, 관련 서비스에 대한 보안이 있는데, 관련 서비스란 네트워크와 시스템, 공공기관, 컴퓨터 비상 대응팀(CERTs)과 컴퓨터 보안사고 대응팀(CSIRTs), 전자통신 네트워크와 서비스를 제공하는 자, 보안기술과 보안서비스 제공자가 제공하거나 이들을 통해 접근 가능한 서비스를 의미한다. 여기에는 전자통신네트워크로의 무단접근과 악성코드배포를 막는 것과 '서비스 거절'공격과 컴퓨터와 전자통신 시스템의 손상을 막는 것이 포함된다.

(50) 원래 수집 목적 이외의 개인정보 처리는 해당 개인정보의 처리가 원래의 수집 목적과 양립 가능한(compatible) 경우에 한해서만 허용되어야 한다. 목적이 양립 가능한 경우, 원래 정보수집을 허용한 법적 근거 이외의 별도의 법적 근거는 불필요하다. (목적이 양립가능하다면 별다른 근거 없이도 추가적으로 정보처리가 가능하다.)
공익 추구를 위하여나, 정보처리자 공적 권한으로 직무를 수행하는 과정에서 개인정보처리가 필요한 경우, 유럽연합·회원국은 법률로써 추가적 정보처리가 양립가능하고 합법적으로 인정될 수 있는 직무와 목적을 결정하고 구체화하여야 한다. 공익상 기록보존의 목적, 과학 및 역사적 연구의 목적, 통계적 목적으로 행하는 추가적인 개인정보 처리는, 양립가능하고 합법적인 처리작업으로 간주되어야 한다. 유럽연합·회원국 법률로써 정하는 개인정보의 처리의 법적 근거 또한 추가적인 정보처리를 위한 법적근거가 되어야 한다.
추가적인 개인정보의 목적이 원래 정보수집의 목적과 양립 가능한지 여부를 확인하기 위하여, 정보처리자는 원래 정보처리의 합법성을 모두 만족시킨 후에 다른 요소를 고려하여야 하는데 그 중에서도: 원래 정보수집의 목적과 추가적 정보처리 목적 간의 연관성이 어떠한지; 개인정보가 수집될 때의 상황, 특히 정보주체가 정보주체와 정보처리자와의 관계를 근거로 할 때 정보의 추가사용이 합리적으로 예측되는지; 개인정보의 성격이 어떤 것인지; 추가적 정보처리의 목적이 정보주체에 어떤 결과를 초래하는지; 원래 정보처리작업과 의도된 추가적 정보처리작업 모두에 대해 적합한 안전장치를 두고 있는 지를 고려하여야 한다.
정보처리자가 목적의 양립가능성 여부와 상관없이 해당 개인정보를 추가적으로 처리할 수 있는 경우가 있는데, 첫째, 정보주체가 동의하였거나, 둘째, 개인정보처리가 민주사회에서의 일반적 공익의 중요한 목표를 보호하는데 필수적이고 비례적인 대책들을 포함하고 있는 유럽연합·회원국의 법률에 근거하여 처리되는 경우이다.

어떤 경우에서도 이 법이 정한 원칙을 준수하여야 하며, 원래 정보처리 목적과 더불어 이의신청권 등 정보주체의 권리를 정보주체에게 통보하여야 한다.
정보처리자가 행하게 될 수도 있는 범죄행위 또는 공안의 위협에 대해 권고하는 것과 개별적·다수 사례에 경우에서 나타나는 해당 범죄행위 또는 공안의 위협에 대한 관련 정보를 관련 기관에 전송하는 것은 정보처리자가 추구하는 정당한 이익에 해당되는 것으로 간주되어야 한다.
그러나 해당 정보처리가 법적, 직무상 또는 기타 구속력 있는 기밀유지의 의무와 양립가능하지 않는 경우, 정보처리자의 정당한 이익을 위한 개인정보 이전 및 추가적 개인정보처리는 금지되어야 한다.

(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.

(52) 특정 범주의 개인정보처리의 금지로부터의 일부제외는 유럽연합 또는 회원국의 법률에 규정되고 적절한 안전장치에 적용받을 경우 허용될 수 있으며, 이는 개인정보와 기타 기본권을 보호하고, 공익에 부합하는 경우 고용법, 연금 등 사회보호법 건강안보, 모니터링, 경계 목적을 위해, 전염병과 건강의 기타 심각한 위협을 예방 또는 통제하기 위함이다. 이러한 일부제외는 공중보건, 의료보장서비스 관리 등 건강 목적을 위해 허용될 수 있으며, 특히 건강보험시스템의 혜택과 서비스에 대한 청구권 처리에 사용되는 절차의 품질과 비용대비 효과를 보장하기 위해서, 또는 공익적인 기록보존 목적, 과학 및 역사연구 목적 또는 통계목적을 위해 허용될 수 있다. 일부제외는 법원 절차로 또는 행정절차나 법원  외의 절차인지 여부와 상관없이, 청구권 입증, 행사 및 방어에 필요한 경우 이러한 개인정보의 처리를 허용할 수

있어야 한다.

(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) 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 건강관련 개인정보의 처리는 고용인 또는 보험사와 금융사 등 제 3자가 기타목적으로 개인정보를 처리하는 결과를 초래하지 않아야 한다.

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

(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) 정보처리자가 본인이 처리하는 개인정보를 통해 개인을 식별하도록 허용하지 않는 경우, 정보처리자는 이 법의 모든 조항을 준수하는 유일한 목적을 위해 정보

주체의 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) 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 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) 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) 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) 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) 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) 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) 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) 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 해

당 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, 정보주체가 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) 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) 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) 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 위해 또는 공익이나 정보처리자에게 부여된 공적권한의 행사를 위한 직무

의 수행에 개인정보가 필요한 경우에는 이 권리가 적용되어서는 안된다. 본인의 개인정보 수령 또는 이전하는 정보주체의 권리가 정보처리자가 기술적으로 양립 가능한 처리 시스템을 채택 또는 유지하도 하는 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) 공익을 위한 업무를 수행하는 경우, 또는 정보처리자에게 부여된 공적 권한 행사나 정보처리자 또는 제 3자의 정당한 이익에 대한 이유로 처리가 필요하여 개인정보가 합법적으로 처리되는 경우에도 불구하고 정보주체는 자신이 처한 특정 상황과 관련해 해당 개인정보처리에 반대할 권리를 갖는다. 정보처리자가 정보처리자의 강력한 정당한 이익이 정보주체의 기본권과 자유 또는 이익을 우선한다는 것을 입증해야 한다.

(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) 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 의사결정은, 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 정

보주체가 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) 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) 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 보호하며, 보관된 개인정보를 이전의 전체주의 정권하의 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) 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. 이

러한 조치는 개인정보처리의 성격, 범위, 상황, 목적 그리고 개인의 권리와 자유에 관한 위험요소를 고려해야 한다.

(75) 개인의 권리와 자유에 관한 위험요소는, 발생가능성과 심각성은 다르지만, 개인정보처리로부터 발생될 수 있으며, 이는 신체적, 물질적, 비(非) 물질적 손상을 초래할 수 있으며, 특히: 처리는 차별, 신용도용 및 신용사기, 재정적 손실, 명예훼손, 직무상의 기밀로 보호되던 개인정보의 기밀성 상실, 가명처리에 대한 무단 재식별 처리, 또는 기타의 심각한 경제적 또는 사회적 불이익을 초래할 수 있는 경우; 정보주체가 본인의 권리와 자유를 빼앗길 수 있는 경우나, 본인의 개인정보에 대한 통제권을 행사하지 못하게 되는 경우; 개인정보가 인종 및 민족의 출신, 정견, 종교 및 철학적 신념, 노동조합의 가입여부와 유전자정보, 건강정보 또는 성생활 관련 정보나 범죄 기소 및 범죄관련 개인정보에 대한 처리 또는 관련 보안 조치를 드러내는 방식으로 처리되는 경우; 개인적인 측면이 업무능력, 경제상황, 건강, 개인의 성향 및 관심사, 신뢰성 또는 행동, 위치 또는 이동성을 개인의 프로파일을 생성 및 활용하기 위해 분석하고 예측하여, 평가되는 경우; 아동 등, 취약한 개인의 개인정보가 처리되는 경우, 또는 처리가 방대한 양의 개인정보와 관련 있거나, 수많은 정보주체에게 영향을 미치는 경우.

(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.

(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) 개인정보의 처리에 관련된 개인의 권리와 자유를 보호하는 것은 이 법의 요건을 충족하기 위해 취해진 적절한 기술 및 관리조치를 요구한다. 이 법을 준수하고 있음을 입증하기 위해, 정보처리자는 개인정보보호 중심 디자인 및 설정의 원칙을 충족하는 내부 정책과 조치를 채택하고 시행해야 한다. 이러한 조치는 개인정보처리의 최소화, 가능한 빠른 시일 내의 개인정보의 가명처리, 개인정보의 기능 및 처리의 투명성 제고, 정보주체의 개인정보처리에 대한 감시와 정보처리자의 보안 대

책의 수립 및 개선으로 구성될 수 있다. 개인정보처리에 근거하거나 관련 업무를 위해 개인정보를 처리하는 어플리케이션, 서비스 및 제품을 개발, 디자인, 선택 및 이용할 때, 해당 제품, 서비스 및 어플리케이션의 제작자는 관련 제품, 서비스 및 어플리케이션을 개발하고 디자인할 때 개인정보보호권을 고려하고 정보처리자와 수탁처리자가 개인정보보호 의무를 준수할 수 있도록 보장하도록 권장된다. 개인정보보호 중심 디자인 및 설정의 원칙은 공개입찰 상황에서도 고려되어야 한다.

(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) 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 정보주체의 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) 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 공인인증메커니즘에 대한 준수는 정보처리자의 의무의 준수를 입증하는 요소로 이용될 수 있다. 수탁처리자의 개인정

보처리의 수행은 유럽연합 또는 회원국 법률에 규정된 계약 또는 기타 법률에 적용받아야 하며, 이를 통해 수탁처리자는 정보처리자에게 구속되고, 처리 주제 및 처리 기간, 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 파기해야 하지만, 수탁처리자가 적용받는 유럽연합 또는 회원국 법률에 따라 개인정보를 보관하라는 요구사항이 있는 경우는 예외로 한다.

(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) 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) 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 이루어져야한다.

(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 통지 내용과 제공되고 관련 정보는 추가적 지체 없이 단계별로 제공될 수 있다..

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

(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) 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) 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.

(93) 공공기관 또는 공공기구의 업무 수행의 근간이 되고 특정 처리방식이나 해당

되는 일련의 처리방식들을 규제하는 회원국의 법률을 채택하는 상황에서, 회원국은 처리 활동에 앞서 개인정보보호 영향 평가를 수행할 필요가 있다고 생각할 수 있다.

(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) 수탁처리자는, 필요 시 또는 요청에 따라, 개인정보보호 영향평가의 수행에서 파생되거나 감독기관의 사전 자문에서 파생되는 의무를 준수하기 위해 정보처리자를 도와야 한다.

(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) 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 지식을 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 본

인의 업무와 임무를 수행해야 한다.

(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) 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) 이 법의 준수와 투명성을 강화하기 위해서, 인증 메커니즘, 개인정보보호 인장및 마크의 수립이 권장되어야 하며, 이를 통해 정보주체는 관련 제품 및 서비스에 대한 개인정보보호의 수준을 빠르게 평가할 수 있다.

(101) 국제교역과 국제협력의 확대를 위해서 유럽연합 역외국가 및 국제기구 간의 개인정보 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.

(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) 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 국제기구

로의 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) 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) 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) 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) 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) 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) 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) 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) 정보주체가 명백한 동의를 제공한 경우이거나 정보이전이 간헐적이고 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) 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) 정보주체의 이익이나 권리 및 자유가 정보처리자가 추구하는 정당한 이익에 우선하지 않는 경우로서 정보처리자가 개인정보 이전과 관련된 모든 정황을 평가했을 때, 간헐적이고 한정된 숫자의 정보주체에 관한 정보이전이 정보처리자가 추구하는 정당한 이익을 강제할 목적으로 가능할 수도 있다. 정보처리자는 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 적정한 안전조치를 특히 고려해야 한다. 이 같은 정보이전은 정보이전을 위한 기타 근거가 적용 가능하지 않은 나머지 경우에서만 가능하다. 과학 및 역사적 연구의 목적 또는 통계의 목적으로, 지식의 증진이라는 사회의 합당한 기대 또한 고려되어야 한다. 정보처리자는 정보이전에 대하여 감독기관 및 해당 정보주체에 고지해야 한다.

(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) 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) 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 국제 협력 메커니즘의 개발을 목적으로, 집행위원회와 감독기구는 호혜를 바탕으로 본 규정을 준수하여 정보를 교환하고 권한 행사와 관련된 활동에 있어 제3국의 주무당국과 협력하여야 한다.

(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) 감독기관의 독립성은 해당 감독기관이 재정지출이나 사법심사와 관련한 통제 또는 모니터링의 대상이 될 수 없다는 것을 의미하지 않는다.

(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) 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 공공 예산을 받아야 하는데 이 예상은 전체 국가 예산의 일부일 수 있다.

(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.

(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) 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) 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. 각료이사회는 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) 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) 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) 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 감

독기관이 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) 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.

(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 사법기관에 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) 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) 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) 일반을 대상으로 한 감독기관의 인식제고 활동에는 교육 분야의 개인과 영세기업·중소기업 등의 정보처리자와 수탁처리자에 초점을 맞춘 특정 조치들이 포함되어야 한다.

(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) 각 감독기관은 적절한 경우 다른 감독기관들과의 공동 작업에 참여해야 한다. 요청을 받은 감독기관은 특정 기한 내에 요청에 응답할 의무가 있다.

(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.

(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) 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) 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) 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 개인정보 처리에 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) 유럽정보보호이사회는 유럽개인정보보호담당기구(European Data Protection Supervisor)가 제공하는 사무처의 지원을 받아야 한다. 본 규정에 의해 유럽정보보호이사회에 부관된 업무를 수행하는 유럽 개인정보보호담당기구의 직원들은 오로지 유럽정보보호이사회 의장의 지시에 따라 업무를 수행하고 의장에게 보고해야 한다.

(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 민원

의 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) 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) 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 감독기관들은 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 국가법정에 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) 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 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) 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) 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 수탁처리자

는 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) 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.

(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) 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) 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.

(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) 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) 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) 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) 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 고용계약의 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) 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 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·관

리적 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) 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) 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 체제하의 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.

(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) 역사적 연구 목적으로 개인정보가 처리되는 경우, 본 규정은 그 같은 정보처

리에도 적용되어야 한다. 여기에는 본 규정이 망자에는 적용되지 않아야 한다는 점을 유념하여 역사 연구 및 계보학 목적의 연구도 포함되어야 한다.

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

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

(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) 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) 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) 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) 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 충족시키는 데 필요한 것 이상을 요구하지 않는다.

(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.

(172) 유럽개인정보보호담당기구는 규정서 (EC) No 45/2001 제28조(2)에 따라 자문을 의뢰받았고 2012년 3월 7일 의견서를 전달하였다.

(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.

본 규정을 채택하였음:

제I장
일반 규정

제1조
주제 및 목적

1. 본 규정은 개인정보의 처리에 관련된 개인의 보호에 관한 규칙 및 개인정보의

자유로운 이동에 관한 규칙에 대해 규정한다.

2. 본 규정은 자연인의 기본권과 자유, 특히 개인정보 보호에 대한 권리를 보호한다.

3. 유럽 내에서의 개인정보의 자유로운 이동이 개인정보의 처리와 관련하여 개인의 보호를 이유로 제한되거나 금지되어서는 안 된다.

제2조
실질적 범위

1. 본 규정은 자동화 수단에 의한 전체적 또는 부분적인 개인정보 처리와 자동화 수단 이외에 의한, 파일링 시스템의 일부를 구성하거나, 구성할 의도가 있는 개인정보 처리에 적용된다.

2. 본 규정은 다음의 각 호에 해당하는 개인정보 처리에는 적용되지 않는다.

(a) 유럽연합 법률의 범위를 벗어나는 활동의 과정인 경우;

(b) 회원국이 TEU의 제V편의 제2장의 범위에 속하는 활동을 수행하는 경우;

(c) 개인이 순수한 개인활동이나 가정활동을 하는 과정의 경우;

(e) 공안의 보호 및 공안에 대한 위협의 예방을 비롯하여 감독기관이 범죄의 예방이나 수사, 적발, 기소 및 형사 처벌의 집행을 위해 처리하는 경우;

3. 유럽연합의 산하기관나 기구, 사무소, 기관에 의한 개인정보처리에는 규정(EC) No 45/2001가 적용된다. 이러한 개인정보 처리에 적용 가능한 규정(EC) No 45/2001 및 기타 유럽연합 법률은 제 98조에 따라 본 규정의 원칙과 규칙에 맞게 변경되어야 한다.

4. 본 규정은 지침(Directive) 2000/31/EC, 특히 해당 지침 제12조에서 제15조까지의 조문에서 규정한 중개서비스사업자(intermediary service provider)의 책임 규정의 적용을 침해하지 않아야 한다.

제3조
영토의 범위

1. 본 규정은 유럽연합 역●내외의 처리 여부에 관계 없이 유럽연합 내의 정보처리자 또는 수탁처리자의 사업장의 활동에 따른 개인정보 처리에 적용된다.

2. 본 규정은, 개인정보의 처리가 다음 각 호에 관련된 경우, 유럽연합 내에 설립되지 않은 정보처리자 또는 수탁처리자에 의한 유럽연합 내에 거주하는 정보주체의 개인정보 처리에 적용된다.

(a) 유럽연합 내의 정보주체에게, 정보주체의 지불 여부와 관계없이, 재화나 서비스를 제공하는 경우; 또는,

(b) 유럽연합 안에서 발생하는 것에 한하여 정보주체의 행동을 감시하는 경우.

3. 본 규정은 유럽연합 내에 설립되지 않았지만, 국제 공법에 의해 회원국의 법률이 적용되는 곳에 설립된 정보처리자에 의한 개인정보의 처리에 적용된다.

제4조
정의

본 규정의 목적을 위해 다음과 같이 정의한다:

(1) '개인정보'는 식별된 또는 식별 가능한 개인('정보주체')과 관련된 일체의 정보를 의미한다. 식별 가능한 개인이란 직접 또는 간접적으로, 특히 이름이나 식별번호, 위치 정보, 온라인 식별자, 또는 해당 개인의 신체나 생리, 유전자, 정신, 경제, 문화 또는 사회적 정체성에 국한된 하나 이상의 요인을 참조하여 식별될 수 있는 자이다.

(2) '처리'는 자동화 수단의 사용 여부에 관계 없이 수집이나 기록, 조직, 구성, 저장, 개조, 변경, 검색, 참조, 사용, 이전을 통한 제공, 배포, 기타 제공, 조화 또는 결합, 제한, 삭제, 파기와 같이 개인정보 또는 일련의 개인정보(sets of personal data)에 수행되는 작업 또는 일련의 작업의 일체를 의미한다.

(3) '처리 제한'은 향후 처리를 제한할 목적으로, 저장된 개인정보에 표시하는 행위를 의미한다.

(4) '프로파일링'은 개인에 관한 특정한 개인적 측면을 평가하기 위해, 특히 개인의 업무능력, 경제 상황, 건강, 개인의 성향이나 관심사, 신뢰도, 행동, 위치, 이동에 관한 측면을 분석 및 예측하기 위해 개인정보를 사용하는 모든 개인정보의 자동처리

형태를 의미한다.

(5) '가명처리'는 추가 정보의 사용 없이 더 이상 특정 정보주체를 식별할 수 없는 방식으로 수행된 개인정보의 처리를 의미하며, 이 경우, 해당 추가정보는 별도로 보관되며 개인정보가 식별된 또는 식별 될 수 있는 개인에게 해당되지 않도록 보장하기 위한 기술 및 관리조치가 적용된다.

(6) '파일링 시스템'이란 개인정보가 기능적 또는 지리적 기준에서 중앙화, 분권화 또는 분산되었는지의 여부와 관계 없이 특정한 기준에 따라 접근할 수 있는 구조화된 일련의 개인정보를 의미한다.

(7) '정보처리자(controller)'란 개인정보의 처리 목적 및 수단을 단독 또는 제 3자와 공동으로 결정하는 자연인 또는 법인, 공공 기관, 관청, 기타 단체 등을 의미한다. 이러한 처리의 목적 및 수단이 유럽연합 또는 회원국 법률에 의해 결정되는 경우, 정보처리자 또는 정보처리자 지명을 위한 특정 기준은 유럽연합 또는 회원국 법률에서 규정될 수 있다;

(8) '수탁처리자(processor)'란 정보처리자를 대신하여 개인정보를 처리하는 자연인 또는 법인, 공공기관, 관청 또는 기타 단체를 의미한다.

(9) '수령인'은 제3자의 여부를 불문하고 개인정보를 제공 받는 자연인이나 법인, 공공기관, 기구, 기타 기구를 의미한다. 그러나 유럽연합이나 회원국 법률에 따라 특정 조회업무의 프레임워크 안에서 개인정보를 수령 받을 수 있는 공공기관은 수령인으로 간주할 수 없다. 해당 공공기관에 의한 개인정보의 처리는 처리 목적에 따라 적용되는 개인정보 보호규칙을 준수해야 한다.

(10) '제3자'는 정보주체와 정보처리자, 수탁처리자, 정보처리자나 수탁처리자의 직접적인 권한에 따라 개인정보를 처리할 수 있는 개인을 제외한 모든 자연인이나 법인, 공공기관, 기구를 의미한다.

(11) '동의'는 진술 또는 명백한 긍정적인 행위를 통해 본인의 개인정보의 처리에 동의함을 나타내는 정보주체의 희망을 자유롭게 제공하고, 구체적이고, 이해하며, 명확하게 나타낸 표시를 의미한다.

(12) '개인정보 유출'은 사고적 혹은 불법적 파기, 손실, 변경, 이전, 보관 또는 다른 작업으로 처리 된 개인정보의 무단 제공 또는 무단 열람을 초래하는 보안 위반을 의미한다.

(13) '유전자 정보'는 개인의 생리 또는 건강에 관한 특정 정보를 제공하며 특히 관련 개인의 생물학적 샘플 분석에서 얻은 결과로 개인의 선천적 또는 후천적인 유전자 특성과 관련된 개인정보를 의미한다.

(14) '생체정보'는 안면 영상이나 지문 정보와 같이 개인 고유의 식별을 허용 또는 확인하는 해당 개인의 신체, 생리, 행동 특성에 관한 특정 기술 처리로 발생하는 개인정보를 의미한다.

(15) '건강관련 정보'는 의료 서비스의 제공을 비롯하여 개인의 건강 상태에 관한 정보를 나타내는 개인의 신체 또는 정신 건강에 관한 개인 정보를 의미한다.

(16) '주 사업장'은 다음 각 호를 의미한다.

(a) 하나 이상의 회원국에 사업장을 지닌 정보처리자와 관련한 경우, 주 사업장은 유럽연합 내의 정보처리자의 중앙 행정장소지만, 개인정보의 처리 목적 및 수단에 관한 결정이 정보처리자의 유럽연합 내 또 다른 사업장에서 발생하는 경우, 또는 후자의 사업장이 이러한 결정을 이행할 권한을 지니고 있는 경우는 예외로 하며, 이 경우 이러한 결정을 한 사업장이 주 사업장으로 간주된다.

(b) 하나 이상의 회원국에 사업장을 지닌 수탁처리자의 경우, 주 사업장은 유럽연합 내의 수탁처리자의 중앙 행정장소거나, 수탁처리자가 유럽연합 내 중앙 행정을 두고 있지 않는 경우에 주 사업장은, 수탁처리자가 본 규정의 특정 의무에 적용 받는 범위에서, 수탁처리자의 사업장 활동 중 주요 처리활동이 발생하는 유럽연합 내 수탁처리자의 사업장이다.

(17) '대리인'은 제27조에 따라 정보처리자 또는 수탁처리자에 의해 서면으로 지정된 유럽연합 내 위치한 자연인 또는 법인을 의미하며, 대리인은 본 규정의 각 정보처리자 및 수탁처리자의 의무와 관련하여 이들을 대신한다.

(18) '기업'은 정기적으로 경제 활동에 종사하는 합명회사 또는 조합 등, 법적 형식에 관계 없이 경제 활동에 종사하는 모든 자연인이나 법인을 의미한다.

(19) '사업체 집단(group of undertakings)'이란 관리 사업체와 피관리 사업체들을 의미한다.

(20) '의무적 기업규칙(binding corporate rules)'은 공동 경제활동에 종사하는 사업체 집단이나 기업집단 안에서 단일의 또는 복수의 제3국에 위치한 정보처리자나 수탁처리자에게 개인정보를 이전하기 위해 회원국 영토에 설립된 정보처리자 또는 수

탁처리자가 준수하는 개인정보 보호정책을 의미한다.

(21) '감독기관'은 제51조에 따라 회원국이 설립한 독립적 공공기관을 의미한다.

(22) '관련 감독기관'은 다음의 사유로 개인정보의 처리에 관여하는 감독기관을 의미한다.
(a) 정보처리자나 수탁처리자가 해당 감독기관의 회원국 영토에 설립되는 경우
(b) 감독기관이 소재한 회원국에 거주하는 정보주체가 처리로 인하여 상당한 영향을 받거나 그럴 가능성이 있을 경우
(c) 해당 감독기관에 민원이 제기된 경우

(23) '회원국간 처리(cross-border processing)'은 다음 중 하나를 의미한다.
(a) 정보처리자 또는 수탁처리자가 하나 이상의 회원국에 설립된 경우, 유럽연합 내의 정보처리자 또는 수탁처리자가 속한 하나 이상의 회원국 안의 사업장의 활동 중 발생하는 개인정보의 처리, 또는

(b) 유럽연합 내의 정보처리자 또는 수탁처리자의 단일 사업장의 활동 중 발생하였지만 하나 이상의 회원국의 정보주체에게 상당히 영향을 주거나 그럴 가능성이 있는 개인정보의 처리.

(24) '타당하고 합당한 이의제기(objection)'는 본 규정의 침해여부나 정보처리자 또는 수탁처리자의 예상되는 행위의 규정 준수 여부에 대한 이의제기를 의미하며, 이는 정보주체의 기본권과 자유와 관련한 결정의 초안, 또는 해당하는 경우, 유럽연합 내의 개인정보의 자유로운 이동으로 초래되는 위험의 유의성을 명확하게 입증한다.

(25) '정보사회 서비스'는 유럽의회 및 각료이사회 지침(EU) 2015/2535의 제1조 (1)항의 (b)에서 정의하는 하나의 서비스를 의미한다.

(21) '국제기구'는 공공국제법이 준용되는 조직 및 산하 기구, 또는 둘 이상의 국가 간의 협정에 의해 또는 이를 기반으로 설립되는 모든 기타 기구를 의미한다.

제II장
원칙

제5조
개인정보 처리 관련 원칙

1. 개인정보는:

(a) 정보주체와 관련하여 합법적으로, 공정하게 그리고 투명한 방식으로 처리되어야 한다("적법성, 공정성, 투명성")

(b) 명시적이며 적법한 특정 목적을 위해 수집되고 해당 목적과 양립하지 않는 방식으로 추가적 처리 되어서는 아니된다; 공익적인 기록보존 목적 또는 과학 및 역사 연구 또는 통계 목적을 위한 추가적 개인정보처리는 제 89조 (1)항에 따라 최초의 목적과 양립되지 않는다고 간주되지 않는다("목적 제한")

(c) 개인정보가 처리되는 목적과 관련하여 적절하고 타당하고 필요한 범위로 제한되어야 한다("데이터 최소화").

(d) 정확하고, 필요 시, 최신의 정보여야 한다; 처리 목적과 관련하여 부정확한 개인정보는 지체 없이 삭제 또는 정정되도록 합리적인 일체의 조치가 취해져야 한다("정확성").

(e) 개인정보의 처리목적에 필요한 기간에 한해서 정보주체가 식별될 수 있는 형태로 보관되어야 한다, 개인정보는, 정보주체의 권리와 자유를 보호하기 위해 본 규정에서 요구하는 적절한 기술 및 관리조치를 규정하는 제89조 (1)항에 따라 공익적인 기록보존 목적 또는 과학 및 역사연구 목적이나 통계목적에 한해 개인정보를 처리하는 경우, 해당 개인정보는 보유기간을 연장할 수 있다 ("보관기간 제한").

(f) 적절한 기술 및 관리조치를 이용하여, 무단(unauthorized) 또는 불법적 처리나 사고로 인한 손실이나 파기, 손상에 대한 보호조치를 포함한 개인정보의 적절한 보안을 보장하는 방식으로 처리해야 한다("무결성"과 "기밀성").

2. 정보처리자는 제1항의 준수를 책임지고 이에 대한 준수를 입증할 수 있어야 한다("책임성").

제6조
처리의 적법성

1. 개인정보 처리는 다음 중 하나 이상이 적용되는 경우에만 적법하다:

(a) 정보 주체가 하나 이상의 특정 목적을 위해 본인의 개인정보 처리에 동의를 제공한 경우;

(b) 정보주체가 계약 당사자로 있는 계약의 이행을 위해 또는 계약 체결 전 정보주

체의 요청에 따라 조치를 취하기 위해 처리가 필요한 경우;

(c) 정보처리자에 적용되는 법적 의무를 준수하는데 처리가 필요한 경우;

(d) 정보주체 또는 제3자의 생명에 관한 이익을 보호하기 위해 처리가 필요한 경우;

(e) 공익 상의 이유 또는 정보처리자에게 부여된 공식권한의 행사를 위한 업무 수행에 처리가 필요한 경우;

(f) 개인정보의 보호를 의무화하는 정보주체의 이익이나 기본권 및 자유가 해당 이익에 우선하지 않는 한, 특히 정보주체가 아동일 경우, 정보처리자나 제3자가 추구하는 정당한 이익의 목적으로 개인정보처리가 필요한 경우.

첫 항의 (f)는 공공기관이 해당 기관 업무의 수행을 위해 진행하는 처리에는 적용되지 않는다.

2. 회원국은 개인정보 처리를 위한 구체적 요건 및 제IX장에 규정된 기타 특정한 정보처리 상황 등 적법하고 공정한 정보처리를 보장하기 위한 기타 조치를 더욱 엄밀히 결정함으로써 (c) 및 (e)에 부합한 개인정보의 처리에 대해 본 규정의 규칙의 적용을 변경하기 위해 더 구체적인 조문을 유지하거나 도입할 수 있다.

3. 제1항의 (c) 및 (e)에 규정된 처리의 근거는 다음 각 호를 통해 규정되어야 한다.

(a) 유럽연합 법률;

(b) 정보처리자에 적용되는 회원국의 법률.

처리목적은 상기의 법적 근거에 의해 결정되거나, 제1항의 (e)에 규정된 처리에 관련한 처리 목적은 공익 또는 정보처리자에게 부여된 공식 권한의 행사를 위한 업무수행을 위해 필요하다. 해당 법적 근거는 본 규정의 규칙 적용을 변경하기 위한 특정 조문을 포함할 수 있다. 특히, 정보처리자가 수행하는 처리의 적법성에 대한 일반적인 조건, 해당 처리에 적용되는 개인정보의 유형, 관련 정보주체, 관련 개인정보가 제공될 수 있는 목적 및 제공받는 대상, 목적 제한, 보관기간, 제IX장에 규정된 기타 특정 처리작업을 위한 조치 등, 적법하고 공정한 처리를 준수하기 위한 조치를 포함한, 처리 작업 및 처리 절차가 포함된다. 유럽연합 또는 회원국 법률은 공익의 목적을 충족하고 추구하는 합법적 목표에 비례해야 한다.

4. 당초 수집목적 이외의 목적으로의 처리가 정보주체의 동의나 제23조 (1)항에 규

정된 목적을 보호하기 위해 민주사회에 필요하고 이에 비례하는 조치를 구성하는 유럽연합 또는 회원국의 법률에 근거하지 않는 경우, 정보처리자는 다른 목적으로의 처리가 당초의 수집 목적과 양립하는 지 여부를 확인하기 위해 특히 다음의 각 호를 고려해야 한다.

수집목적과 예정된 추가 처리 목적 간의 연관성;

특히 정보주체와 정보처리자의 관계와 관련하여 개인 정보가 수집된 상황;

개인 정보의 성격. 특히 제9조에 따라 특정 범주의 개인정보의 처리 여부, 또는 제10조에 따라 범죄경력 및 범죄 행위와 관련한 개인정보의 처리 여부;

예정된 추가 처리가 정보 주체에 초래할 수 있는 결과;

(e) 암호처리 및 가명처리가 포함될 수 있는 적절한 보호수단의 유무..

제7조
동의 조건

1. 처리가 동의를 기반으로 하는 경우, 정보처리자는 정보주체가 본인의 개인정보 처리에 동의를 제공하였음을 입증할 수 있어야 한다.

2. 기타 사안과도 관련이 있는 서면 선언의 맥락에서 정보주체가 동의를 제공하는 경우, 동의에 대한 요청은 기타 사안과 명확하게 구분되는 방식으로, 이해하기 쉽고 손쉽게 접근할 수 있는 양식으로 명확하고 평이한 문구가 이용되어 제시되어야 한다. 본 규정을 침해하는 선언은 구속력을 갖지 않는다.

3. 정보주체는 언제든지 본인의 동의를 철회할 권리를 갖는다. 동의의 철회는 철회 이전에 동의를 기반으로 하는 처리의 적법성에 영향을 미치지 않는다. 정보주체는 동의를 제공하기 전에 이에 대해 고지 받아야 한다. 동의의 철회는 동의의 제공만큼 용이해야 한다.

4. 동의가 자유 의사에 따라 제공되었는지 평가하는 경우, 특히 서비스의 제공을 비롯한 계약의 이행이 본 계약 이행에 필요하지 않은 정보 처리에 대한 동의를 조건으로 하는지 면밀히 고려해야 한다.

제8조

정보 사회 서비스에 관한 아동의 동의에 적용되는 조건
1. 정보 사회 서비스를 아동에게 직접 제공하는 경우와 관련하여 제6조 (1)항의 (a)가 적용될 경우, 아동이 16세 이상인 경우, 아동의 개인정보처리는 적법하다. 아동이 16세 미만인 경우, 해당 아동에 대해 부모의 책임을 지는 자가 동의를 제공하거나 허가하는 경우에만 적법성을 갖는다.

회원국은 상기의 목적으로 아동의 나이를 법으로 낮추어 규정할 수 있으나, 13세 미만으로 규정할 수는 없다.

2. 정보처리자는 이러한 경우, 가용한 기술을 참작하여, 해당 동의가 관련 아동에 대해 부모의 책임을 지는 자가 제공 또는 허가하였는지 증명하기 위해 합당한 노력을 기울인다.

3. 제1항은 아동과 관련된 계약의 유효성, 형식, 효과에 대한 규정 등, 회원국의 일반 계약법률에 영향을 미쳐서는 안 된다.

제9조
특정범주의 개인정보 처리

1. 인종이나 민족, 정견, 종교나 철학적 신념, 노조 가입여부가 드러나는 개인정보의 처리와 유전자정보 또는 개인을 특정하게 식별할 수 있는 생체정보, 또는 건강정보, 성생활, 성적 취향에 관한 정보의 처리는 금지된다.

2. 다음 각 호에 해당하는 경우에는 제1항은 적용되지 않는다

(a) 정보 주체가 단일 또는 복수의 특정 목적으로 특정범주의 개인정보를 처리하는데 명백한 동의를 제공한 경우. 단, 유럽연합 또는 회원국 법률에서 제1항에 규정된 금지조문을 정보주체가 철회할 수 없다고 명시하는 경우는 제외된다.

(b) 정보주체의 기본권 및 이익에 대해 적절한 안전장치를 제공하는 회원국 법률에 따른 단체협약이나 유럽연합 또는 회원국 법률이 허용하는 범위에서, 고용, 사회안보와 사회보호법 분야에서 정보처리자 또는 정보주체의 특정권리를 행사하고 이들의 의무를 수행하기 위한 목적으로 처리가 필요한 경우;

(c) 정보주체가 물리적 또는 법률적으로 동의를 제공할 수 없는 경우로 정보주체 또는 다른 사람의 생명과 관련된 이익을 보호하는 데 필요한 경우;

(d) 정치적, 철학적, 종교적 또는 노동조합의 목적을 지닌 재단, 조합, 비영리기관이

적절한 안정 조치를 갖추어 수행하는 합법적인 활동의 과정에서, 그리고 해당 처리가 그 목적에 맞게 관련 기관의 회원 또는 이전 회원 또는 관련 단체와 정기적으로 접촉하는 사람에 한하여 관련된다는 조건과, 정보주체의 동의 없이 이러한 개인정보를 기관 외부에 제공하지 않는다는 조건에 따른 합법적 활동의 과정에서 처리가 수행되는 경우;

(e) 정보주체가 명백히 공개한 개인정보를 처리하는 경우;

(f) 청구권의 입증이나 행사, 또는 방어를 목적으로, 또는 법원이 사법능력을 행사하는 때마다 처리가 필요한 경우

(g) 개인정보보호권의 본질을 존중하고 정보주체의 기본권 및 이익을 보호하기 위해 적절하고 구체적인 조치를 제공하며, 추구하는 목적에 비례하는 유럽연합 또는 회원국 법률에 근거하여, 중요한 공익상의 이유로 처리가 필요한 경우,

(h) 유럽연합 법률이나 회원국 법률, 의료전문가와의 계약, 제3항에 규정된 조건 및 안전조치에 따라 예방의학이나 직업의학의 목적으로 또는 직원의 업무능력 평가나 의학적 진단, 의료나 사회복지 및 치료의 제공, 또는 의료나 사회 복지 제도 및 서비스의 관리를 위해 처리가 필요한 경우;

(i) 직무상 기밀 등, 정보주체의 권리와 자유를 보호하기 위해 적절하고 구체적인 조치를 규정하는 유럽연합 또는 회원국 법률에 근거하여, 회원국 간 중대한 건강위협으로부터 보호하거나 높은 수준의 의료 품질 및 안전성과 의약품이나 의학장비를 보장하기 위함 등, 공중보건 분야에서 공익 상의 이유로 처리가 필요한 경우;

(i) 개인정보보호권의 본질을 존중하고 정보 주체의 기본권 및 이익을 보호하는데 적합한 구체적인 대책을 규정하며 추구하는 목적에 적절한 유럽연합이나 회원국 법률에 따라 제83조 (1)에 부합하는 공익적인 기록보존 목적이나 과학 및 역사 연구 목적, 또는 통계 목적을 위해 처리가 필요한 경우.

(j) 추구하는 목적에 비례하고 개인정보보호권의 본질을 존중하며 정보주체의 기본권 및 이익을 보호하기 위해 적절하고 구체적인 조치를 규정하는 유럽연합 또는 회원국 법률에 근거한 제 89조 (1)항에 따라, 공익상의 기록보관 목적이나 과학 및 역사 연구 목적, 또는 통계목적을 위해 처리가 필요한 경우.

3. 제1항에 언급된 개인정보는 해당 개인정보가 유럽연합 또는 회원국 법률이나 국가 관련기관이 수립한 규정에 따른 직무상 비밀 의무를 적용 받는 전문가의 책임에 의해 또는 책임 하에 처리되는 경우, 또는 유럽연합 또는 회원국 법률이나 관련 국

가기관에 수립한 규정에 따른 비밀의 의무에 적용 받는 또 다른 개인에 의해 이러한 개인정보가 처리되는 경우, 제2항의 (h)에 규정된 목적을 위해 처리될 수 있다.

4. 회원국은 유전자정보나 생체정보, 건강정보와 관련하여, 제한을 포함한 추가 조건을 유지 또는 도입할 수 있다.

제10조
범죄경력 및 범죄행위에 관한 개인정보의 처리

범죄경력 및 범죄 행위 또는 제6조 (1)항에 근거한 안보조치와 관련한 개인정보의 처리는 공공기관의 규제 하에서만 수행될 수 있거나, 해당 처리가 정보주체의 권리와 자유를 위한 적절한 안전조치를 규정하는 유럽연합 또는 회원국 법률에 승인되는 경우 수행될 수 있다.. 종합 전과 기록은 공공 기관의 규제 하에서만 보관될 수 있다.

제11조
신원확인을 요하지 않는 개인정보의 처리

1. 정보처리자가 개인정보를 처리하는 목적상 정보처리자가 정보주체의 신원확인을 요구하지 않거나 더 이상 요구하지 않아도 되는 경우, 정보처리자는 본 규정을 준수할 목적에 한하여 정보 주체를 식별하기 위한 추가 정보를 유지 또는 취득 또는 처리할 의무를 지지 않는다.

2. 본 조문의 제1항에 규정된 경우, 정보처리자가 직위상, 정보주체를 식별할 수 없다는 것을 증명할 수 있는 경우, 정보처리자는 가능하면 이 사실을 정보주체에 통지한다. 이 경우, 제15조에서 20조까지의 조문은 적용되지 않으며, 해당 조문에 따라 본인의 권리를 행사하기 위한 목적으로 정보주체가 본인의 신원을 확인할 수 있는 추가적 정보를 제공하는 경우는 예외로 한다.

제III장
정보주체의 권리

제1절
투명성 및 형식

제12조
정보주체의 권리 행사하기 위한 투명한 정보, 통지 및 형식.

1. 정보처리자는 개인정보 처리와 관련한 제13조 및 제14조에 규정된 일체의 정보와 제15조에서 제22조까지의 조문 그리고 제34조에 따른 모든 통지를, 특히 아동에게 제공하는 경우, 간결하고 투명하고 이해하기 쉽고 손쉽게 접근할 수 있는 양식에 명확하고 평이한 언어를 사용하여 제공하기 위해 적절한 조치를 취해야 한다. 해당 정보는 서면이나 적절한 경우, 전자수단 등 기타 수단을 이용하여 제공되어야 한다. 정보주체가 요청하는 경우, 다른 수단을 통해 정보주체의 신원이 입증되면, 해당 정보는 구두로 제공될 수 있다.

2. 정보처리자는 제15에서 제20조까지의 조문에 따라 정보주체의 권리 행사를 용이하게 해야 한다. 제11조의 (2)항에 규정된 상황의 경우, 정보처리자는 제15조에서 제22조까지의 조문에 따른 본인의 권리를 행사하기 위한 정보주체의 요청을 거절해서는 안되며, 정보처리자가 정보주체를 식별할 수 있는 위치가 아님을 입증하는 경우는 예외로 한다.

3. 정보처리자는 요청을 접수 받은 후, 한 달 안에 부당한 지체 없이, 제15조에서 제22조까지의 조문에 따른 요청에 따라 취해진 조치에 대한 정보를 제공해야 한다. 해당 요청의 복잡성과 요청 횟수를 참작하여 필요한 경우 해당 기간을 2개월 간 더 연장할 수 있다. 정보처리자는 요청을 접수 받은 지 한 달 이내에, 정보주체에게 연기 사유와 함께 연장기간에 대해 고지한다.. 정보주체가 전자 양식의 수단으로 요청을 하는 경우, 정보주체가 별도의 다른 요청이 있지 않는 한, 해당 정보는 가능한 경우 전자양식으로 제공되어야 한다..

4. 정보처리자가 정보주체의 요청에 대해 조치를 취하지 않을 경우, 정보처리자는 지체없이, 요청을 접수 받은 후 한 달 이내에 조치를 취하지 않은 사유와 감독기관에 민원을 제기하고 사법 구제를 구할 수 있는 가능성을 정보주체에게 고지한다.

5. 제13조 및 제14조에 규정된 정보와 제15조에서 제22조까지의 조문 및 제34조 조문에 따른 일체의 통지 및 조치는 무료로 제공되어야 한다. 정보주체의 요청이 명백하게 근거가 없거나 과도한 경우, 특히 요청이 반복될 경우, 정보처리자는 다음 중 하나의 방법을 취할 수 있다.

관련 정보나 통지를 제공하거나 요청한 조치를 취하기 위한 행정적 비용을 참작한 합리적인 요금을 부과한다.

해당 요청에 대한 응대를 거부한다.

정보처리자는 해당 요청이 명백하게 근거가 없거나 과도하다는 사실을 입증할 책임

이 있다.

6. 제15조에서 제19조까지의 조문에 규정된 요청을 하는 개인의 신원과 관련하여 합리적인 의심이 드는 경우, 정보처리자는 제11조를 침해하지 않고 정보주체의 신원을 확인하는데 필요한 추가적 정보의 제공을 요청할 수 있다.

7. 제13조 및 제14조에 따라 정보주체에게 제공되는 정보는 눈에 띄고 이해하기 쉽고 가독성이 뛰어난 방식으로 예정된 처리의 의미 있는 개괄설명을 제공하기 위해 표준화된 아이콘과 함께 제공될 수 있어야 한다. 해당 아이콘이 전자 방식으로 제공되는 경우, 이는 기계 판독이 가능해야 한다.

8. 집행위원회는 아이콘이 보여주는 정보와 표준 아이콘을 제공하는 절차를 결정하기 위한 목적으로 제92조에 따라 위임 법률을 채택할 권한을 갖는다.

제2절
정보 및 개인정보 열람

제13조
정보주체로부터 개인정보를 수집하는 경우, 제공되는 정보

1. 정보주체에 관련된 개인정보를 정보주체로부터 수집하는 경우, 정보처리자는 개인정보를 취득할 당시 정보주체에게 다음의 모든 정보를 제공한다.

(a) 정보처리자 또는, 가능한 경우, 정보처리자의 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)항의 (f)에 근거한 처리의 경우, 정보처리자 또는 제3자가 추구하는 정당한 이익;

(e) 해당되는 경우, 개인정보의 수령인 또는 수령인의 범주;

(f) 해당 되는 경우, 정보처리자가 제3국이나 국제기구의 수령인에게 개인정보를 이전할 예정이라는 사실과 집행위원회의 적합성 결정의 유무, 또는 제46조나 제47조, 또는 제49조의 (1)항의 두 번째 단락에 규정된 이전의 경우나 해당 이전이 공개되는 경우, 적절하고 적합한 보호수단과 이에 대한 사본을 입수하기 위한 수단;

2. 제1항에 규정된 정보와 함께, 정보처리자는 개인 정보가 입수될 때 공정하고 투명한 처리를 보장하기 위해 필요한, 다음의 추가 정보를 정보주체에 제공한다.

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

(b) 정보처리자에게 본인의 개인정보에 대한 열람, 수정, 또는 삭제, 또는 정보주체와 관련된 처리에 대한 제한이나 처리에 대한 반대를 요청할 수 있는 권리와 본인의 개인정보 이전권의 유무;

(c) 해당 처리가 제6조 (1)항의 (a)나 제9조 (2)항의 (a)에 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 법률이나 계약상의 요건이거나 계약 체결에 필요한 요건일 뿐 아니라 정보주체가 개인정보를 제공할 의무가 있는 지의 여부 및 해당 정보를 제공하지 않을 경우 발생할 수 있는 결과;

(f) 제22조의 (1)항 및 (4)항에 규정된 프로파일링 등, 자동 의사결정의 유무 또한 최소한 이 경우, 관련 논리에 관한 유의미한 정보와 이러한 정보주체에 대한 처리의 유의성과 예상되는 결과;

3. 정보처리자가 개인정보의 수집 목적 이외의 목적으로 개인정보를 추가적 처리를 할 예정인 경우, 정보처리자는 추가적 처리 이전에, 정보주체에게 기타의 해당 목적에 관한 정보와 제2항에 규정된 모든 관련된 추가적 정보를 제공한다.

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

제14조

정보주체로부터 개인정보가 수집되지 않은 경우 제공되는 정보

1. 개인정보가 정보주체로부터 수집되지 않은 경우, 정보처리자는 다음의 정보를 정보주체에게 제공한다.

(a) 정보처리자 또는, 가능한 경우, 정보처리자의 대리인의 신원 및 상세 연락처;

(b) 해당되는 경우, 개인정보보호 담당관의 상세 연락처;

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

(d) 관련 개인정보의 범주;

(e) 해당되는 경우, 개인정보의 수령인 또는 수령인의 범주;

(f) 해당 되는 경우, 정보처리자가 제3국이나 국제기구의 수령인에게 개인정보를 이전할 예정이라는 사실과 집행위원회의 적합성 결정의 유무, 또는 제46조나 제47조, 또는 제49조의 (1)항의 두번째 단락에 규정된 이전의 경우나 해당 이전이 공개되는 경우, 적절하고 적합한 보호수단과 이에 대한 사본을 입수하기 위한 수단;

2. 제1항에 규정된 정보와 함께, 정보처리자는 정보주체와 관련한 공정하고 투명한 처리를 보장하기 위해 필요한, 다음의 정보를 정보주체에 제공한다.

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

(b) 제6조 (1)항의 (f)에 근거한 처리의 경우, 정보처리자 또는 제3자가 추구하는 정당한 이익;

(c) 정보처리자에게 본인의 개인정보에 대한 열람, 수정, 또는 삭제, 또는 정보주체와 관련된 처리에 대한 제한이나 처리에 대한 반대를 요청할 수 있는 권리와 본인의 개인정보 이전권의 유무;

(d) 해당 처리가 제6조 (1)항의 (a)나 제9조 (2)항의 (a)에 근거하는 경우, 철회 이전에 동의를 기반으로 하는 처리의 적법성에 영향을 주지 않고 언제든지 동의를 철회할 수 있는 권리의 유무;

(e) 감독기관에 민원을 제기할 수 있는 권리;

(f) 개인 정보의 제공이 법률이나 계약상의 요건이거나 계약 체결에 필요한 요건일 뿐 아니라 정보주체가 개인정보를 제공할 의무가 있는 지의 여부 및 해당 정보를 제공하지 않을 경우 발생할 수 있는 결과;

(g) 제22조의 (1)항 및 (4)항에 규정된 프로파일링 등, 자동 의사결정의 유무 또한 최소한 이 경우, 관련 논리에 관한 유의미한 정보와 이러한 정보주체에 대한 처리의 유의성과 예상되는 결과;

3. 정보처리자는 제1항 및 제2항에 규정된 정보를 다음과 같이 제공해야 한다.

(a) 개인정보가 처리된 특정 상황과 관련하여 개인정보를 입수 한 후 합리적인 기간 내로, 최소한 한 달 이내;

(b) 개인정보가 정보주체에게로의 통지 목적으로 이용되는 경우, 최소한 해당 정보주체에 최초로 통지한 시점;

(c) 제3의 수령인에게 개인정보의 제공이 예상되는 경우, 최소한 개인정보가 최초로 제공되는 시점;

4. 정보처리자가 취득 목적 이외의 목적으로 개인정보를 추가적 처리를 하려는 경우, 해당 정보처리자는 추가적 처리 이전에 정보주체에게 해당 기타의 목적에 대한 정보와 제2항에 규정된 관련의 추가적 정보의 일체를 제공한다.

5. 제1항에서 제4항까지의 모든 조항은 다음의 경우 적용되지 않는다.

(a) 정보주체가 이미 해당 정보를 보유하고 있는 경우;

(b) 제89조 (1)항에 규정된 조건 및 안전조치에 따라, 공익 상의 기록보관 목적이나 과학 및 역사연구 목적 또는 통계목적으로의 처리에 대해, 해당 정보의 제공이 불가능하거나 과도한 노력이 수반되어야 하는 경우, 또는 본 조문의 제1항에 규정된 의무가 불가능하다고 생각되거나 관련 처리의 목적 달성을 심각하게 저해하는 경우. 이러한 경우, 정보처리자는 해당 정보의 공개 등, 정보주체의 권리와 자유 그리고 정당한 이익을 보호하기 위해 적절한 조치를 취해야 한다;

(c) 정보처리자에 적용되며, 정보주체의 정당한 이익을 보호하는데 적절한 조치를 규정하는 유럽연합 또는 회원국 법률에서 취득과 제공을 명백하게 규정하는 경우; 또는

(d) 개인정보가 법정 비밀유지 의무 등, 유럽연합 또는 회원국 법률에 의해 규제되는 직무상 기밀의 의무에 따라, 해당 개인정보가 기밀로 남아있어야 하는 경우;

제15조
정보주체의 열람권

1. 정보주체는 본인에 관련된 개인정보의 처리 여부에 관련해 정보처리자로부터 확인을 획득할 권리를 가지며, 이 경우, 개인정보 및 다음의 정보에 대한 열람권을 갖는다.

(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 결정하기 위해 이용되는 기준;

(e) 정보처리자에게 본인의 개인정보에 대한 수정, 또는 삭제, 또는 정보주체와 관련된 처리에 대한 제한이나 처리에 대한 반대를 요청할 수 있는 권리의 유무;

(f) 감독기관에 민원을 제기할 수 있는 권리;

(g) 개인정보가 정보주체로부터 수집되지 않은 경우, 개인정보의 출처에 대한 모든 가용한 정보;

(h) 제22조의 (1)항 및 (4)항에 규정된 프로파일링 등, 자동 의사결정의 유무 또한 최소한 이 경우, 관련 논리에 관한 유의미한 정보와 이러한 정보주체에 대한 처리의 유의성과 예상되는 결과;

2. 개인정보가 제3국이나 국제기구에 이전되는 경우, 정보주체는 제46조에 따라 거절한 안전조치에 대해 고지 받을 의무가 있다.

3. 정보처리자는 진행 중인 처리의 개인정보의 사본을 제공해야 한다. 정보주체가 추가의 사본을 요청하는 경우, 정보처리자는 행정적 비용에 근거한 합리적인 비용

을 청구할 수 있다. 정보주체가 전자 방식으로 해당 요청을 하는 경우, 관련 정보는 일반적으로 사용되는 전자 양식으로 제공되어야 한다.

4. 제3항에 규정된 사본을 입수할 권리는 다른 개인들의 권리와 자유를 침해하지 않아야 한다.

제3절
수정 및 삭제

제16조
수정권

정보주체는 본인에 관한 개인 정보에 대해 정확하지 않은 부분을 부당한 지체 없이 수정하도록 정보처리자에게 요구할 권리를 갖는다. 정보주체는 처리목적을 참작하여 추가 진술을 제공할 수단을 통하는 등, 부족한 개인정보의 부분을 채울 수 있는 권리를 갖는다.

제17조
삭제권("잊힐 권리")

1. 정보주체는 본인에 관한 개인정보의 삭제를 정보처리자에게 요청할 권리를 가지며, 정보처리자는 다음의 각 호가 적용되는 경우, 부당한 지체 없이 개인정보를 삭제할 의무를 갖는다.

(a) 개인정보가 수집 목적 또는 다른 방식으로 처리되는 목적에 더 이상 필요하지 않은 경우;

(b) 정보주체가 제6조 (1)항의 (a) 또는 제9조 (2)항의 (a)에 따른 처리의 기반이 되는 동의를 철회하고 해당 처리에 대한 기타의 법적 사유가 없는 경우;

(c) 정보주체가 제21조 (1)항에 따라 관련 처리에 반대하고 관련 처리에 대해 우선하는 정당한 사유가 없거나, 정보주체가 제21조 (2)항에 따라 처리에 반대하는 경우;

(d) 개인정보가 불법적으로 처리된 경우;

(e) 개인정보가 정보처리자에 적용되는 유럽 또는 회원국 법률의 법적 의무를 준수하기 위해 삭제되어야 하는 경우;

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

2. 정보처리자가 개인정보를 공개하고 제1항에 따라 해당 개인정보를 삭제할 의무가 있는 경우, 정보처리자는 가용한 기술과 시행 비용을 참작하여 개인정보를 처리하는 정보처리자에게 정보주체가 이러한 개인정보를 처리하는 정보처리자들에게 관련된 개인정보에 대한 링크, 사본 또는 재현물의 삭제를 요청했음을 알리기 위한 기술적 조치 등, 합리적인 조치를 취해야 한다.

3. 제1항 및 제2항은 다음 각 호와 같이 처리가 필요한 경우 적용되지 않는다.

(a) 표현과 정보의 자유에 대한 권리의 행사;

(b) 정보처리자에 적용되는 유럽연합 또는 회원국 법률의 처리를 요구하는 법적 의무를 준수하기 위해 또는 공익 상의 업무를 수행하기 위해 또는 정보처리자에게 부여된 공적 권한을 행사하기 위해;

(c) 제9조 (2)항의 (h) 및 (i)뿐 아니라 제9조 (3)항에 따라 공중 보건 분야의 공익상의 이유인 경우;

(d) 89조 (1)항에 따라 공익 상의 기록보존 목적이나 과학 또는 역사연구 목적 또는 통계목적으로, 제1항에 규정된 권리가 불가능하다고 생각되거나 해당 처리의 목적 달성을 심각하게 저해할 가능성이 있는 경우; 또는,

(e) 청구권의 입증이나 행사, 방어를 위한 경우.

18조
처리에 대한 제한권

1. 정보주체는 다음 각 호의 경우, 정보처리자로부터 처리에 대한 제한권을 획득할 수 있다.

(a) 정보처리자가 개인정보의 정확성을 증명할 수 있는 기간 동안, 정보주체가 해당 개인정보의 정확성에 대해 이의를 제기하는 경우;

(b) 처리가 불법적이고 정보주체가 해당 개인정보의 삭제에 반대하고 대신 개인정보에 대한 이용제한을 요청하는 경우

(c) 정보처리자가 처리목적으로 해당 개인정보가 더 이상 필요하지 않으나, 정보처리자가 청구권의 입증이나 행사, 방어를 위해 요구하는 경우;

(d) 정보주체가 정보처리자의 정당한 이유가 정보주체의 정당한 이유에 우선하는지 여부를 확인할 때까지, 정보주체가 제21조 (1)항에 따른 처리에 대해 반대하는 경우

2. 개인정보의 처리가 제1항에 따라 제한되는 경우, 해당 정보는, 보관을 제외하고, 정보주체의 동의가 있거나 청구권의 입증이나 행사, 방어를 위해, 또는 제3의 자연인이나 법인의 권리의 보호를 위하거나 유럽연합 또는 회원국의 주요한 공익 상의 이유에 한하여 처리될 수 있다.

3. 제1항에 따라 처리의 제한을 취득한 정보주체는 처리제한이 해제되기 전에 정보처리자로부터 이를 고지 받을 수 있다.

19조
개인정보의 수정이나 삭제 또는 처리의 제한에 관한 고지 의무

정보처리자는 개인정보를 제공 받은 각 수령인에게 제16조, 17조의 (1)항 또는 제18조에 따른 개인정보의 수정이나 삭제 또는 처리의 제한에 대해 통지해야 하며, 이러한 통지가 불가능하거나 과도한 노력을 수반하는 경우는 예외로 한다. 정보처리자는 정보주체가 요청 시, 정보주체에게 해당 수령인에 대해 통지한다.

제20조
본인의 개인정보 이전권
1. 정보주체는 정보처리자에게 제공한 본인에 관련된 개인정보를 체계적으로 작성되고 일반적으로 사용되며 기계 판독이 가능한 형식으로 수령 받을 권리가 있으며, 개인정보를 제공 받은 정보처리자를 방해하지 않고 다른 정보처리자에게 해당 개인정보를 이전할 권리를 갖는다.

(a) 제6조 (1)항의 (a)나 제9조 (2)항의 (a)에 따른 동의나 제6조 (1)항의 (b)에 따른 계약을 기반으로 하는 처리의 경우;

(b) 자동 수단을 통해 처리가 수행되는 경우.

2. 제1항에 따른 본인의 개인정보 이전권을 행사하는 데 있어, 기술적으로 가능한 경우, 정보주체는 해당 개인정보를 한 정보처리자에서 다른 정보처리자로 직접 이

전하게 할 권리를 갖는다.

3. 본 조문의 제1항에 규정된 권리의 행사는 제17조를 침해해서는 아니된다. 해당 권리는 공익 상의 업무를 수행하기 위해 또는 정보처리자에게 부여된 공식 권한의 행사를 위해 필요한 처리에는 적용되지 않는다.

4. 제1항에 규정된 권리는 다른 개인의 권리와 자유를 침해하지 않아야 한다.

제4절
반대할 권리 및 자동 개별 의사결정

제21조
반대할 권리
1. 정보 주체는 언제든지 본인의 특정 상황에 대한 이유로 제6조 (1)항의 (e) 및 (f)에 근거한 프로파일링 등, 본인과 관련한 개인정보의 처리에 대해 언제든지 반대할 권리를 갖는다. 정보처리자는 정보주체의 이익, 권리 및 자유에 우선하는 처리, 또는 청구권의 입증이나 행사, 또는 방어를 위한 강력하고 정당한 이유를 입증하지 않는 한, 개인정보를 더 이상 처리할 수 없다.

2. 직접 마케팅을 목적으로 개인정보가 처리되는 경우, 정보주체는 언제든지 해당 마케팅을 위한 본인에 관한 개인 정보의 처리에 반대할 권리가 있으며, 해당 직접 마케팅과 관련된 경우에는 프로파일링이 포함된다.

3. 정보주체가 직접 마케팅을 위한 처리에 반대하는 경우, 해당 개인정보는 이러한 목적으로 더 이상 처리될 수 없다.

4. 제1항 및 제2항에 규정된 권리는, 최소한 정보주체에게 처음 고지한 시점에, 명백하게 정보주체에게 통지되어야 하며, 명백하고 다른 기타 정보와는 별도로 제공되어야 한다.

5. 정보 사회 서비스 이용의 맥락에서, 지침 2002/58/EC에도 불구하고, 정보주체는 기술적 세부사항을 이용하는 자동화 수단을 통해 이에 반대할 권리를 행사할 수 있다.

6. 제89조 (1)항에 따라 과학 또는 역사연구 목적 또는 통계 목적으로 개인정보가

처리되는 경우, 정보주체는 본인의 특정 상황과 관련한 이유로, 본인에 관련된 개인정보의 처리에 반대할 권리를 갖는다. 단, 해당 처리가 공익 상의 이유로 이행되는 업무의 수행을 위해 필요한 경우는 예외로 한다.

제22조
프로파일링을 비롯한 자동 개별 의사결정
1. 정보주체는 프로파일링 등, 본인에 관한 법적 효력을 초래하거나 이와 유사하게 본인에게 중대한 영향을 미치는 자동 처리에만 의존하는 결정의 적용을 받지 않을 권리를 갖는다.

2. 결정이 하기 각 호에 해당하는 경우에는 제1항이 적용되지 않는다.

(a) 정보주체와 정보처리자 간에 계약을 체결 또는 이행하는데 필요한 경우;

(b) 정보처리자에 적용되며, 정보주체의 권리와 자유, 정당한 이익을 보호하기 위한 적절한 조치에 대해 규정하는 유럽연합 또는 회원국 법률이 허용하는 경우;

(c) 정보주체의 명백한 동의에 기반하는 경우.

3. 제2항의 (a) 및 (c)에 규정된 경우, 정보처리자는 정보주체의 권리 및 자유와 정당한 이익, 최소한 정보처리자의 인적 개입을 확보하고 본인의 관점을 피력하며 결정에 대해 이의를 제기할 수 있는 권리를 보호하는데 적합한 조치를 시행해야 한다.

4. 제2항에 규정된 결정은 제9조의 (1)항에 규정된 특정 범주의 개인정보에 기반해서는 아니된다. 단, 제9조 (2)항의 (a)와 (g)가 적용되고 또한 정보주체의 권리와 자유, 정당한 이유를 보호하는 적절한 조치가 시행되는 경우는 예외로 한다.

제5절
제한

제21조
제한

1. 해당 제한이 기본권과 자유의 본질을 존중하고 민주사회에서 하기 다음의 각호를 보호하는 데 필요하고 비례적인 조치인 경우, 정보처리자 또는 수탁처리자에 적용되는 유럽연합 또는 회원국 법률은 입법 조치를 통해 제12조에서 제22조까지의 조문과 제34조뿐 아니라 제5조의 조항이 제12조에서 제22조까지의 조문에 규정된

권리와 의무에 부합하는 경우, 제5조에서 규정하는 의무와 권리의 범위를 제한할 수 있다.

(a) 국가안보;

(b) 국방;

(c) 공공 안보(public security);

(d) 공안의 보호 및 공안에 대한 위협의 예방을 비롯한 범죄의 예방이나 수사, 적발, 기소, 형사 처벌의 집행;

(e) 유럽연합 또는 회원국에 일반 공익상의 기타의 중요한 목표, 특히 통화나 예산, 과세 현안 또는 공중보건 및 사회보장 등, 유럽연합 또는 회원국에 중요한 경제적 또는 재정적 이익;

(f) 사법 독립성 및 사법 절차에 대한 보호

(g) 규제되는 직업(regulated professions)의 윤리 침해에 대한 예방, 조사, 적발, 기소;

(h) 본 항의 (a), (b), (c), (d), (e), (g)에서 규정된 경우, 공적 권한의 행사에 대한 간헐적인 모니터링,조사(inspection) 또는 규제기능;

(i) 정보주체 또는 제3자의 권리와 자유에 대한 보호;

(j) 민법 청구의 집행.

2. 특히, 제1항에 규정된 모든 법적 조치에는 최소한, 관련 있는 경우, 다음 각 호에 관한 구체적인 조항이 포함되어야 한다.

(a) 처리 목적이나 처리 범주;

(b) 개인정보의 범주;

(c) 도입된 제한의 범위;

(d) 남용이나 불법 열람이나 이전을 예방하기 위한 안전조치;

(e) 정보처리자의 상세조항 또는 정보처리자의 범주;

(f) 저장 기간 및 관련 처리의 성격, 범위, 목적 또는 처리의 범주를 고려한 안전조치;

(g) 정보주체의 권리 및 자유에 대한 위험;

(h) 제한의 목적을 침해하지 않는 한, 정보주체가 제한에 관한 정보를 고지 받을 권리.

제IV장
정보처리자와 수탁처리자

제1절
일반적인 의무

제24조
정보처리자의 책임

1. 정보처리자는 처리의 성격과 범위, 상황, 목적뿐 아니라 개인의 권리와 자유의 변경 가능성과 중대성의 위험성을 참작하여, 개인정보의 처리가 본 규정을 준용하여 수행되는 것을 보장하고 이를 입증할 수 있는 적절한 기술 및 관리조치를 이행한다. 이러한 조치는, 필요 시, 검토되고 업데이트 되어야 한다.

2. 처리활동과 관련하여 비례하는 경우, 제1항에 규정된 조치는 정보처리자의 적절한 개인정보보호 정책의 이행을 포함해야 한다.

3. 제40조에 규정된 공인된 행동강령의 준수 또는 제42조에 규정된 공식 인증 메커니즘은 정보처리자의 의무의 준수를 입증하기 위한 요소로 이용될 수 있다.

제25조
개인정보보호 중심 디자인 및 설정

1. 최신 기술과 실행 비용, 처리의 성격과 범위, 상황, 목적뿐 아니라 처리로 인해 개인의 권리와 자유에 대해 발생할 수 있는 변경 가능성과 중대성의 위험성을 참작하여, 정보처리자는 처리 수단을 결정한 시점과 처리 당시 시점에서, 데이터 최소화 등 개인정보보호의 원칙을 이행하고 본 규정의 요건을 충족하고 정보주체의 권리를

보호하기 위해, 처리에 필요한 안전조치를 포함하기 위해 고안된 가명처리 등, 적절한 기술 및 관리조치를 이행해야 한다.

2. 정보처리자는 기본설정을 통해, 처리의 개별 특정목적에 필요한 정도에 한하여 개인정보가 처리될 수 있도록 보장하기 위한 적절한 기술 및 관리조치를 이행해야 한다. 이러한 의무는 수집되는 개인정보의 양, 해당 처리의 범위, 개인정보의 보관기간 및 접근용이성에 적용된다. 특히, 이러한 조치는 개인정보가 관련 개인의 개입 없이 불특정 다수에게 열람되지 않도록 기본설정을 통해 보장한다.

3. 제42조에 근거한 공식 인증 메커니즘은 본 조항의 제1항 및 제2항에 규정된 요건의 준수를 입증하는 요소로 이용될 수 있다.

제26조
공동 정보처리자

1. 두 명 이상의 정보처리자가 공동으로 처리의 목적과 수단을 결정하는 경우, 이들은 공동 정보처리자가 된다. 공동 정보처리자는 당사자간의 합의를 통해, 본 규정에 따른 책임을 준용, 특히 정보주체의 권리 행사에 대한 각자의 책임과 제13조 및 제14조에 규정된 정보를 제공할 각자의 임무를 투명하게 결정해야 하되, 이러한 각자의 책임이 정보처리자에 적용되는 유럽연합 또는 회원국 법률에 의해 결정되는 경우는 예외로 한다. 이 같은 합의로 정보주체에 대한 연락담당관을 지정할 수 있다.

2. 제1항에 규정된 합의는 정보주체에 대한 공동 정보처리자의 개별 역할과 관계를 충분히 반영해야 한다. 해당 합의의 본질은 정보주체에 제공되어야 한다.

3. 제1항에 규정된 합의의 조건과 관계없이, 정보주체는 본 규정에 따라 각정보처리자와관련하여혹은이들에반대하여본인의권리를행사할수있다.

제27조
유럽연합 내에 설립되지 않은 정보처리자 또는 수탁처리자의 대리인

1. 제3조의 (2)항이 적용되는 경우, 정보처리자 혹은 수탁처리자는 유럽연합 역내 대리인을 서면으로 지정한다.

2. 이 의무는 다음의 경우 적용되지 않는다.

(a) 처리가 간헐적으로 이루어지고 대규모의 처리가 아니며, 제9조 (1)항에 규정된 특정범주의 개인정보의 처리, 제10조에 규정된 범죄경력 및 범죄 행위에 관련된 개

인정보의 처리를 포함하지 않거나 처리의 성격, 상황, 범위, 목적을 고려했을 때, 개인의 권리와 자유에 대한 위험을 초래할 가능성이 낮은 처리의 경우; 또는

(b) 공공기관 또는 기구;

3. 대리인은 정보주체가 거주하고, 재화 및 서비스를 제공 받는 것과 관련하여 개인정보가 처리되거나 정보주체의 행동이 모니터링 되는 여러 회원국 중 한 곳에 설립되어야 한다.

4. 대리인은 정보처리자 또는 수탁처리자에 의해 위임되며, 정보처리자 또는 수탁처리자와 함께 또는 이들을 대신하여, 감독기관과 정보주체에 따라, 본 규정을 준수하기 위한 목적으로 처리와 관련한 모든 사안에 착수해야 한다.

5. 정보처리자 또는 수탁처리자의 대리인 지정은 정보처리자 또는 수탁처리자 자신에게 반하여 제기될 수 있는 법적 행동을 침해하지 않아야 한다.

제28조
수탁처리자

1. 정보처리자를 대신하여 처리를 수행하는 경우, 정보처리자는 처리가 본 규정의 요건을 준수하고 정보주체의 권리의 보호를 보장하는 방식으로 적절한 기술 및 관리조치를 이행한다는 충분한 보증을 제공하는 수탁처리자만 이용해야 한다

2. 수탁처리자는 사전의 구체적 또는 일반적인 정보처리자의 서면 승인 없이 다른 수탁처리자와 일을 할 수 없다. 일반적인 서면승인의 경우, 수탁처리자는 정보처리자에게 다른 수탁처리자의 추가영입 또는 대체와 관련한 예정된 변경에 대해 고지하여, 정보처리자가 이러한 변경에 반대할 기회를 제공해야 한다.

3. 수탁처리자가 수행하는 처리는 유럽연합 또는 회원국 법률에 따른 계약이나 기타 법률이 적용 되며, 이를 통해 수탁처리자는 정보처리자에게 구속되고 처리의 주제와 처리기간, 처리의 성격 및 목적, 개인정보의 유형 및 정보주체의 범주와 정보처리자의 권리와 의무가 규정된다. 해당 계약 또는 기타 법률은 특히 수탁처리자에 대해 다음과 같이 규정한다.

(a) 수탁처리자는 정보처리자의 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 정보처리자에게 고지해야 하며, 해당 법률이 공익 상의 중요한 이유로 이러한 통지를 금지하는 경우는 예외로 한다.

(b) 수탁처리자는 개인정보를 처리하도록 승인 받은 개인이 기밀유지를 약속하도록 보장하거나 해당 개인이 적절한 법적 기밀유지의 의무에 적용 받도록 한다.

(c) 제32조에 따라 요구되는 모든 조치를 취한다;

(d) 다른 수탁자와 협력하기 위해서 제2항 및 제4항에 규정된 조건을 존중한다.

(e) 수탁처리자는 해당 처리의 성격을 참작하여, 제III장에 규정된 정보주체의 권리 행사의 요청에 대응해야 하는 정보처리자의 의무의 이행을 위해, 가능한 경우, 적절한 기술 및 관리조치를 통해 정보처리자를 지원한다.

(f) 수탁처리자는 처리의 성격과 수탁처리자에게 가용한 정보를 참작하여, 제32조에서 36조에 따른 의무의 준수를 보장하는 데 있어 정보처리자를 지원한다.

(g) 정보처리자의 선택에 따라, 수탁처리자는 처리와 관련된 서비스의 공급이 종료된 후, 모든 관련 개인정보를 삭제하거나 정보처리자에게 반환하며, 기존 사본을 삭제한다. 유럽연합 또는 회원국 법률이 해당 개인정보의 보관을 요구하는 경우는 예외로 한다.

(h) 본 조문에 규정되는 의무의 준수를 입증하는데 필요한 일체의 정보를 정보처리자에게 제공하고 검사를 비롯하여 정보처리자 또는 정보처리자가 위임한 타 감사자가 수행하는 감사를 허용 및 기여한다.

첫 하위단락의 (h)와 관련하여, 수탁처리자는 어떠한 지시가 본 규정 또는 기타 유럽연합이나 회원국의 개인정보보호 조문을 위반한다고 판단되는 즉시 정보처리자에게 이에 대해 통지한다.

4. 수탁처리자가 정보처리자를 대신하여 특정 처리 활동을 수행하기 위해 타 수탁처리자와 함께 일하는 경우, 제3항에 규정된 정보처리자와 수탁처리자 간의 계약 또는 기타 법률에 규정된 동일한 개인정보보호의 의무는 유럽연합 또는 회원국 법률에 따른 계약이나 기타 법률의 방식으로 관련 타 수탁처리자에게 부과되어야 하며, 특히 해당 처리가 본 규정의 요건을 충족할 수 있는 그러한 방식으로 적절한 기술 및 관리조치를 이행하는 것에 대해 충분한 보증을 제공해야 한다. 해당 타 수탁처리자가 본인의 개인정보 보호의 의무를 이행하지 않을 경우, 최초의 수탁처리자는 기타 처리자의 의무 이행에 대해 정보처리자에게 전적인 책임을 져야 한다.

5. 제40조에 규정된 공인된 행동강령이나 제42조에 규정된 공식 인증 메커니즘에 대한 수탁처리자의 준수는 본 조문의 제1항 및 제4항에 규정된 충분한 보증을 입증하는 요소로 이용될 수 있다.

6. 정보처리자와 수탁처리자 간의 개별 계약을 침해하지 않고, 본 조문의 제3항 및 제4항에 규정된 계약 또는 기타 법률은 일부 또는 전적으로 본 조문의 제7항 및 8항에 규정된 정보보호 표준 계약조항(standard contractual clauses)에 근거할 수 있으며 여기에는 해당 계약 및 기타 법률이 제42조 및 제43조에 따라 정보처리자 또는 수탁처리자에게 수여된 인증의 일부인 경우도 포함된다.

7. 집행위원회는 본 조문의 제3항 및 제4항에 규정된 사안을 위한, 또한 제93조 (2)항에 규정된 심사 절차에 따라 정보보호 표준 계약조항(standard contractual clauses)을 규정할 수 있다.

8. 감독기관은 본 조문의 제3항 및 제4항에 규정된 사안을 위한, 또한 제63조에 규정된 일관성 메커니즘에 따라 정보보호 표준 계약조항(standard contractual clauses)을 채택할 수 있다.

9. 제3항 및 제4항에 규정된 계약이나 기타 법률은 전자 양식을 포함한 서면으로 작성되어야 한다.

10. 제82조, 제83조, 제84조를 침해하지 않고, 수탁처리자가 처리의 목적 및 수단을 결정함으로써 본 규정을 위반하는 경우, 수탁처리자는 해당 처리와 관련하여 정보처리자로 간주된다.

제29조
정보처리자 및 수탁처리자의 권한에 따른 처리

수탁처리자와 정보처리자 또는 수탁처리자의 권한을 대신하여 개인정보를 열람할 수 있는 개인은정보처리자의 지시에 따른 경우를 제외하고 해당 정보를 처리할 수 없으나, 유럽연합 또는 회원국 법률에서 요구하는 경우는 예외로 한다.

제30조
처리 활동의 기록
1. 각 정보처리자와, 가능한 경우, 해당 정보처리자의 대리인은 본인의 책임 하에

진행되는 처리 활동의 기록을 유지해야 한다. 해당 기록은 다음의 정보를 포함해야 한다.

(a) 정보처리자와, 가능한 경우, 공동 정보처리자, 정보처리자의 대리인 및 개인정보 담당관의 이름 및 연락처;

(b) 처리의 목적;

(c) 정보주체의 범주 및 개인정보의 범주에 대한 설명;

(d) 제3국 또는 국제기구의 수령인 등, 개인정보를 제공받았거나 제공 받을 예정인 수령인의 범주;

(e) 가능한 경우, 제3국 및 국제기구의 신원 등, 제3국 또는 국제기구로의 개인정보 이전 사실과 제49조 (1)항의 2호에 규정된 이전의 경우, 적절한 안전조치에 대한 문서;

(f) 가능한 경우, 다른 범주의 개인정보에 대한 삭제에 예상되는 시간;

(g) 가능한 경우, 제32조 (1)항에 규정된 기술 및 관리 안전조치에 대한 일반적인 설명;

2. 각 수탁처리자와, 가능한 경우, 해당 수탁처리자의 대리인은 정보처리자를 대신하여 수행하는 모든 범주의 처리활동에 대한 기록을 유지해야 하며, 해당 기록은 다음의 정보를 포함해야 한다.

(a) 관련 수탁처리자(들)와 수탁처리자가 대행하는 각 정보처리자, 가능한 경우, 정보처리자와 수탁처리자의 대리인 및 개인정보 담당관의 이름 및 연락처;

(b) 각 정보처리자를 대신하여 수행하는 처리의 범주;

(c) 가능한 경우, 제3국 및 국제기구의 신원 등, 제3국 또는 국제기구로의 개인정보 이전 사실과 제49조 (1)항의 2호에 규정된 이전의 경우, 적절한 안전조치에 대한 문서;

(d) 가능한 경우, 제32조 (1)항에 규정된 기술 및 관리 안전조치에 대한 일반적인 설명;

3. 제1항 및 제2항에 규정된 기록은 전자 양식 등, 서면으로 작성되어야 한다.

4. 해당 정보처리자와 수탁처리자, 그리고 가능한 경우, 정보처리자 또는 수탁처리자의 대리인은 요청이 있을 경우 감독기관에 기록을 제공한다.

5. 제1항 및 제2항에 규정된 의무는 직원 250인 미만의 기업이나 조직에는 적용되지 않는다. 단, 해당 기업이 수행하는 처리가 정보주체의 권리와 자유에 위험을 초래할 가능성이 있거나, 간헐적이지 않거나, 제9조 (1)항에 규정된 특정범주의 개인정보를 포함하거나, 제10조에 규정된 범죄경력 및 범죄 행위에 관련된 개인정보를 다루는 경우는 예외로 한다.

제31조
감독기관과의 협력

정보처리자와 수탁처리자, 가능한 경우, 정보처리자나 수탁처리자의 대리인은 직무를 수행함에 있어 감독기관의 요청이 있을 경우 이에 협력해야 한다.

제2절
개인정보의 보안

제32조
처리의 보안

1. 최신 기술, 이행 비용, 처리의 성격과 범위, 상황, 목적뿐 아니라 개인의 권리 및 자유에 대해 발생할 수 있는 변경 가능성과 중대성의 위험성을 참작하여 정보처리자와 수탁처리자는 특히 아래의 조치를 비롯하여 위험에 적합한 보안 수준을 보장하는데 적절한 기술 및 관리조치를 실행해야 한다.

(a) 개인정보의 가명처리 및 암호처리;

(b) 처리 시스템 및 서비스의 지속적 기밀성과 무결성, 가용성, 복원력을 보장할 수 있는 능력.;

(c) 물리적 사고나 기술적 사고가 발생하는 경우 개인정보에 대한 가용성 및 열람을 시의 적절하게 복원 할 수 있는 능력;

(d) 정기적인 검사(testing), 평가 및 해당 처리의 보안을 보장하기 위한 기술 및 관리조치의 효용성에대한 평가를 위한 과정.

2. 적절한 보안 수준을 평가할 때는 처리로 인해 발생하는 위험요소, 특히 이전, 저장 또는 다른 작업으로 처리된 개인정보에 대한 사고적 또는 불법 파기, 손실, 변경, 무단 제공, 무단 열람에 대해 고려해보아야 한다..

3. 제40조에 규정된 공인된 행동강령이나 제42조에 규정된 공식 인증 메커니즘에 대한 준수는 본 조문의 제1항에 규정된 요건의 준수를 입증하는 요소로 이용될 수 있다.

4. 정보처리자와 수탁처리자는 정보처리자나 수탁처리자의 권한에 따라 개인정보를 열람하는 모든 개인이 정보처리자의 지시에 따른 경우를 제외하고는 개인정보를 처리하지 못하도록 보장하며, 해당 개인이 유럽연합 또는 회원국 법률에 요구에 따라 처리한 경우는 예외로 한다.

제33조
감독기관에 대한 개인정보 유출 통지

1. 개인정보의 유출이 발생할 경우, 정보처리자는 부당한 지체 없이, 가급적 이를 알게 된 후 72시간 안에, 제55조에 따라 관련 감독기관에 해당 개인정보의 유출에 대해 통지해야 한다. 단, 해당 개인정보의 유출이 개인의 권리와 자유에 위험을 초래할 가능성이 없는 경우는 예외로 한다. 72시간 안에 감독기관에 이를 통보하지 않을 경우에는 정당한 근거를 동봉해야 한다.

2. 수탁처리자는 개인정보의 유출을 알게 된 후 부당한 지체 없이 정보처리자에게 이를 통보한다.

3. 제1항에서 규정한 통지는 최소한 다음을 포함하여야 한다:

(a) 가능한 경우, 관련 정보주체의 범주 및 대략적인 정보주체의 수와 관련 개인정보 기록의 범주 및 대략적인 개인정보의 수 등, 개인정보 유출의 성격에 대한 설명;

(b) 개인정보보호담당관 및, 더 많은 정보를 얻을 수 있는 경우, 기타 연락 가능한 개인에 대한 이름 및 상세 연락처 전달;

(c) 개인정보 유출로 인해 발생할 수 있는 결과에 대한 설명;

(d) 적절한 경우, 개인정보 유출로 인한 부작용을 완화하기 위한 조치 등, 해당 개인정보 유출 해결을 위해 정보처리자가 취하거나 취하도록 제시된 조치에 대한 설

명.

4. 정보를 동시에 제공할 수 없는 경우에는 부당한 지체 없이 해당 정보를 단계별로 제공할 수 있다.

5. 정보처리자는 개인정보 유출과 관련된 사실, 유출로 인한 영향, 이에 대해 실시된 시정 조치 등, 모든 개인정보 유출 건을 문서화한다.

제34조
정보주체에 대한 개인정보 유출 사실 통지

1. 개인정보의 유출이 개인의 권리와 자유에 대한 중대한 위험을 초래할 가능성이 있는 경우, 정보처리자는 부당한 지체 없이 정보주체에게 개인 정보 유출에 대해 통지한다.

2. 본 조문의 제1항에 규정된 정보주체로의 통지는 해당 개인정보 유출의 성격을 명확하고 평이한 언어로 기술하며 제33조 (3)항의 (b),(c),(d)에 규정된 정보와 권고를 최소한 포함해야 한다.

3. 다음의 조건 중 하나라도 충족되는 경우, 제1항에 규정된 정보주체에게 통지가 의무가 되지 않는다(not required).

(a) 정보처리자가 적절한 기술 및 관리 보호조치를 실행하고, 개인정보 유출로 영향을 받은 개인정보에 상기 조치가 적용되며, 특히 암호처리 등, 해당 개인정보의 열람에 대한 승인을 받지 못한 개인은 해당 정보를 이해하지 못하도록 하는 조치가 적용되는 경우;

(b) 정보처리자가 제1항에 규정된 정보주체의 권리와 자유에 대한 중대한 위험이 실현될 가능성이 없도록 만드는 후속 조치를 취한 경우;

(c) 부당한 노력이 수반될 수 있는 경우. 이 경우, 동등한 효과가 있는 방식으로 정보주체가 알 수 있게 되는 공개 통보나 유사한 조치를 취해야 한다.

4. 정보처리자가 정보주체에게 개인정보 유출에 대해 아직 통지하지 않은 경우, 관련 감독기관은 중대한 위험을 초래할 수 있는 개인정보 유출의 가능성을 고려하여, 통지하도록 하거나, 제3항의 조건이 충족되도록 결정할 수 있다.

제3절
개인정보보호 영향평가 및 사전 자문

제35조
개인정보보호 영향평가

1. 처리의 성격과 범위, 상황, 목적을 참작하여, 특히 신기술을 사용하는 처리 유형이 개인의 권리와 자유에 중대한 위험을 초래할 수 있는 경우, 정보처리자는 정보를 처리하기 전에 개인정보의 보호에 대한 예상되는 처리 작업에 대한 영향평가를 수행해야 한다. 한 번의 평가를 통해 유사한 중대한 위험을 초래하는 비슷한 일련의 처리 작업을 해결할 수 있다.

2. 정보처리자는 개인정보보호 담당관이 지정된 경우, 개인정보보호 영향평가를 수행할 때, 담당관의 조언을 구한다.

3. 제1항에 규정된 개인정보보호 영향평가는 특히 다음 각 호의 경우 요구되어야 한다.

(a) 프로파일링 등의 자동화 처리에 근거한, 개인에 관한 개인적 측면에 대한 체계적이고 광범위한 평가이며 해당 평가에 근거한 결정이 해당 개인에게 법적 효력을 미치거나 이와 유사하게 개인에게 중대한 영향을 미치는 경우;

(b) 제9조 (1)항에 규정된 특정범주의 개인정보에 대한 대규모 처리나 제10조에 규정된 범죄경력 및 범죄 행위에 관련된 개인정보에 대한 처리; 또는

(c) 공개적으로 접근 가능한 지역에 대한 대규모의 체계적 모니터링.

4. 감독기관은 제1항에 따라 개인정보보호 영향평가의 요건이 적용되는 처리 작업의 종류의 목록을 제정 및 공개한다. 감독기관은 제 68조에 규정된 유럽정보보호이사회에 해당 목록을 통보한다.

5. 감독기관은 개인정보보호 영향평가가 요구되지 않는 처리 작업의 종류의 목록 또한 제정 및 공개할 수 있다. 감독기관은 유럽정보보호이사회에 해당 목록을 통보한다.

6. 제4항 및 제5항에 규정된 목록을 채택하기 이전에, 관련 감독기관은 해당 목록이 복수의 회원국 내의 정보주체에게 재화와 서비스를 제공하거나 그들의 행동을 모니터링 하는 것과 관련된 처리활동에 관계가 있는 경우, 또는 유럽연합 내 개인정보

의 자유로운 이동에 중대한 영향을 미칠 수 있는 처리활동과 관련 있는 경우, 제63조에 규정된 일관성 메커니즘을 적용해야 한다.

7. 평가는 최소한 다음의 각 호를 포함해야 한다.

(a) 가능한 경우, 정보처리자가 추구하는 정당한 이익을 포함한 예상되는 처리 작업과 처리 목적에 대한 체계적인 설명;

(b) 목적과 관련한 처리 작업의 필요성과 비례성에 대한 평가;

(c) 제1항에 규정된 정보주체의 권리와 자유에 대한 위험의 평가;

(d) 정보주체 및 기타의 관련 개인의 권리와 정당한 이익을 고려하여, 개인정보보호를 보장하고 본 규정의 준수를 입증하기 위해, 안전조치, 보안조치 및 메커니즘 등, 위험을 해결하기 위해 예상되는 조치.

8. 특히 개인정보보호 영향평가를 위해 관련 정보처리자나 수탁처리자가가 수행하는 처리 작업의 영향을 평가할 때는 해당 정보처리자나 수탁처리자가 제40조에 규정된 공인된 행동강령의 준수여부를 고려해야 한다.

9. 적절한 경우, 정보처리자는 상업적 이익이나 공익의 보호 또는 처리 작업의 보안을 침해하지 않고, 예정된 처리에 대한 정보주체 또는 정보처리자의 대리인의 의견을 구해야 한다.

10. 제6조 (1)항의 (c) 또는 (e)에 따른 처리가 정보처리자에 적용되는 유럽연합 또는 회원국 법률 내에 법적 근거를 두고 있는 경우, 해당 법률은 특정 처리 작업이나 일련의 해당 작업을 규제하고 개인정보보호 영향평가는 해당 법적 근거를 채택하는 상황인 경우, 일반적인 영향평가의 일부로 이미 수행된 것이므로, 제1항에서 제7항까지 적용되지 않는다. 단, 회원국이 처리활동 이전에 이러한 영향평가의 수행이 필요하다고 고려하는 경우는 예외로 한다.

11. 정보처리자는 처리 작업으로 초래되는 위험이 변경되는 경우, 필요한 경우, 처리가 개인정보보호 영향평가에 따라 수행되는 지 여부를 평가하기 위한 검토를 최소한 시행해야 한다.

제36조
사전 자문

1. 제35조에 따라 수행된 개인정보보호 영향평가에서 해당 처리에 위험을 완화하고자 하는 정보처리자의 조치가 부재할 경우, 해당 처리가 중대한 위험을 초래할 수 있다고 하는 경우, 정보처리자는 처리 이전에 감독기관에 자문을 구해야 한다.

2. 감독기관이 제1항에 규정된 예정된 처리가 본 규정을 침해할 수 있다는 의견을 내놓는 경우, 특히 정보처리자가 해당 위험을 충분히 확인하지 못했거나 완화하지 못했다고 판단하는 경우, 해당 감독기관은 자문 요청을 받은 후 최대 팔 주 이내에 정보처리자에게 서면으로 자문을 제공해야 하며, 수탁처리자에게 적용 가능한 경우, 제58조에 규정된 일체의 권한을 행사할 수 있다. 본 기간은 예정된 처리의 복잡성을 참작하여 6주간 추가로 연장할 수 있다. 감독기관은 정보처리자에게, 가능할 경우 수탁처리자에게, 지연된 이유와 함께 자문요청 이후 한 달 이내에 이러한 기간 연장에 대해 통지해야 한다. 해당 기간은 감독기관이 자문 목적으로 요청한 정보를 입수할 때까지 중지될 수 있다.

3. 제1항에 따라 감독기관에 자문을 구하는 경우, 정보처리자는 다음 각 호를 감독기관에 제공해야 한다.

(a) 가능한 경우, 관련 처리에 관련된 정보처리자, 공동 정보처리자 및 수탁처리자의 개별 책임 특히 사업체집단 내의 처리에 대한 책임;

(b) 예정된 처리의 목적 및 수단;

(c) 본 규정에 따라 정보주체의 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.

4. 회원국은 자국 의회가 채택하는 입법 조치에 대한 제안서 또는 이러한 입법 조치에 근거한 처리에 관련된 규제조치를 준비하는 동안 자문기관의 자문을 구한다.

5. 제1항에도 불구하고, 회원국 법률은 사회 보호 및 공중 보건과 관련된 처리 등, 공익을 위해 정보처리자가 진행하는 업무의 수행을 위한 처리와 관련하여, 정보처리자가 감독기관에게 자문을 구하고 사전 승인을 획득하도록 요구할 수 있다.

제4절
개인정보보호 담당관

제37조
개인정보보호 담당관의 지정

1. 다음의 각 호의 경우 정보처리자와 수탁처리자는 개인정보보호 담당관을 지정해야 한다.

(a) 법원이 사법능력을 행사하는 경우를 제외하며, 공공기관 또는 기구에 의해 처리가 수행되는 경우;

(b) 정보처리자나 수탁처리자의 핵심 활동이 처리의 성격과 범위 및/또는 목적 상 정보주체에 대한 정기적이고 체계적인 대규모의 모니터링을 요하는 처리 작업들로 구성되는 경우

(c) 정보처리자 또는 수탁처리자의 핵심 활동이 제9조에 따른 특정범주의 개인정보와 제10조에 규정된 범죄경력 및 범죄 행위에 관련된 개인정보에 대한 대규모의 처리로 구성되는 되는 경우;

2. 개인정보보호 담당관을 각 사업장에서 쉽게 접근할 수 있는 경우, 사업체 집단은 한 명의 개인정보보호 담당관을 임명할 수 있다.

3. 정보처리자 또는 수탁처리자가 공공기관이나 기구인 경우, 조직의 구조나 규모를 고려하여, 이러한 다수의 기관이나 기구를 위해 한 명의 개인정보보호 담당관이 지정될 수 있다.

4. 제1항에 규정되지 않은 경우, 정보처리자 또는 수탁처리자 또는 정보처리자나 수탁처리자의 범주를 대변하는 조합 및 기타 기구는, 유럽연합 또는 회원국 법률에서 요구하는 경우, 개인정보보호 담당관을 지정할 수 있거나 지정해야 한다. 개인정보보호 담당관은 정보처리자 또는 수탁처리자 대변하는 해당 조합 및 기타 기구를 대행할 수 있다.

5. 개인정보보호 담당관은 직무상의 자질, 특히 개인정보보호법과 실무에 대한 전문가적 지식과 제39조에 규정된 업무를 수행할 수 있는 능력에 근거하여 지정된다.

6. 개인정보보호 담당관은 정보처리자 또는 수탁처리자의 직원일 수 있으며, 서비스 계약에 근거하여 업무를 수행할 수 있다.

7. 정보처리자 또는 수탁처리자는 개인정보보호 담당관의 상세 연락처를 발표하며 이를 관련 감독기관에 통보한다.

제38조
개인정보보호 담당관의 지위

1. 정보처리자 및 수탁처리자는 개인정보보호 담당관이 개인정보 보호와 관련된 모든 문제에 시의적절하고 적절하게 관여하도록 보장한다.

2. 정보처리자 및 수탁처리자는 이러한 업무의 수행뿐 아니라 개인정보에 대한 열람 및 처리 작업들에 대한 접근을 위한 전문지식을 유지하는데 필요한 자료를 제공하여 제39조에 규정된 업무를 수행하는 데 있어 개인정보보호 담당관을 지원해야 한다.

3. 정보처리자 또는 수탁처리자는 개인정보보호 담당관이 본 업무의 실행에 관한 어떠한 지시도 받지 않도록 보장해야 한다. 개인정보보호 담당관은 본인의 업무 수행을 이유로 정보처리자나 수탁처리자에 의해 해임 또는 처벌받아서는 아니된다. 개인정보보호 담당관은 정보처리자 또는 수탁처리자의 최고 경영진에게 직접 보고한다.

4. 개인정보보호 담당관은 유럽연합이나 회원국 법률에 따라 본인의 직무 수행에 관해 비밀 또는 기밀유지의 의무를 준수해야 한다.

5. 개인정보보호 담당관은 기타 업무 및 직무를 수행할 수 있다. 정보처리자나 수탁처리자는 이러한 업무 및 직무가 이해의 상충을 초래하지 않도록 보장해야 한다.

제39조
개인정보보호 담당관의 업무

1. 개인정보보호 담당관은 최소한 아래의 업무를 수행한다.

(a) 정보처리자나 수탁처리자, 그리고 처리를 수행하는 해당 직원에게 본 규정과 유럽연합 또는 회원국의 개인정보보호 조문에 따른 의무에 대해 고지하고 조언한다.

(b) 본 규정, 기타 유럽연합 또는 회원국의 개인정보보호 조문과 개인정보보호와 관련한 정보처리자 또는 수탁처리자의 정책의 준수에 대해 모니터링을 하며, 여기에

는 책임 배정, 인식 제고, 처리 작업에 관련된 직원 교육과 관련 감사 등이 포함된다.

(c) 요청이 있을 경우, 제35조에 따라 개인정보보호 영향평가에 관한 자문을 제공하고 평가의 이행을 감시한다.

(d) 감독기관에 협력한다.

(e) 제36조에 규정된 사전 자문 등, 처리에 관련한 현안에 대해 감독기관의 연락처의 역할을 수행하고 적절한 경우, 기타 사안에 대해 자문을 제공한다.

2. 개인정보보호 담당관은 업무를 수행할 때 처리의 성격과 범위, 상황, 목적을 참작하여 처리 작업과 관련한 위험을 충분히 고려해야 한다.

제5절
행동강령 및 인증

제40조
행동강령

1. 회원국과 감독기관, 유럽정보보호 이사회, 집행위원회는 다양한 처리 부문의 구체적인 특징과 영세 기업과 중소기업의 구체적인 요구를 참작하여 본 규정의 적절한 적용에 기여하기 위한 행동강령의 입안을 장려한다.

2. 정보처리자나 수탁처리자의 범주를 대변하는 조합과 기타 기구는 다음과 관련하여, 본 규정의 적용을 명시할 목적으로 행동강령을 작성하거나 해당 강령을 개정 또는 확대할 수 있다.

(a) 공정하고 투명한 처리;

(b) 특정 상황에서 정보처리자가 추구하는 정당한 이익;

(c) 개인정보의 수집;

(d) 개인정보의 가명처리;

(e) 일반 대중 및 정보주체에게 제공되는 정보;

(f) 정보주체의 권리 행사;

(g) 아동에게 제공되는 정보, 아동에 대한 보호와 부모의 책임을 지닌 자의 아동에 관련한 동의를 취득할 수 있는 방식;

(h) 제24조 및 제25조에 규정된 조치와 절차와 제32조에 규정된 처리의 보안을 보장하기 위한 조치;

(i) 감독기관 및 정보주체에게 개인정보 유출에 대해 통지;

(j) 제3국이나 국제기구로 개인정보 이전;

(k) 제77조 및 제79조에 따른 정보주체의 권리를 침해하지 않고, 처리와 관련하여 정보처리자와 정보주체 간의 분쟁을 해결하기 위한 재판 외 절차와 기타 분쟁 해결 절차.

3. 본 규정에 적용 받는 정보처리자 또는 수탁처리자의 준수와 더불어, 제3조에 따라 본 규정에 적용 받지 않는 정보처리자 또는 수탁처리자는 제46조 (2)항 (e)에 규정된 조건에 따라 제3국 또는 국제기구로의 개인정보 이전에 대한 프레임워크 안에서 적절한 안전조치를 제공하기 위해 본 조문의 제5항에 따라 공인된 행동강령과 본 조문의 제9항에 따른 일반적인 효력을 갖는 행동강령을 준수할 수 있다. 해당 정보처리자 또는 수탁처리자는 계약 증서 또는 기타의 법적 구속력이 있는 증서를 통해, 정보주체의 권리를 비롯하여 상기의 적절한 안전조치를 적용하기 위해 구속력과 강제력 있는 약정을 작성해야 한다.

4. 본 조문의 제2항에 규정된 행동강령은 제41조 (1)항에 규정된 기구가 제55조와 제56조에 따른 감독기관의 업무와 권한을 침해하지 않고, 행동강령을 적용하는 정보처리자와 수탁처리자가 해당 조문을 준수하는 지 여부에 대한 의무적인 모니터링을 수행하는 메커니즘을 포함해야 한다.

5. 행동강령을 작성하거나 기존 강령을 개정 또는 확대할 의도인 본 조문의 제2항에 규정된 조합 또는 기타 기구는 제55조에 따른 감독기관에 강령 초안이나 개정 또는 확대 강령을 제출해야 한다. 감독기관은 강령 초안이나 개정 또는 확대 강령이 본 규정에 부합하는지 의견을 제시하고 적절한 보호 수단을 제공한다고 판단되는 경우, 해당 초안이나 개정 또는 확대 강령을 승인한다.

6. 강령 초안이나 개정 또는 확대 강령이 제5항에 따라 승인되는 경우, 또한 해당 행동 강령이 여러 회원국의 처리 활동과 관련되지 않을 경우, 감독기관은 강령을

등록 및 발표한다.

7. 행동강령 초안이 여러 회원국의 처리 활동에 관련될 경우, 제55조에 따른 관련 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 준수하는 지 여부, 또는 제3항에 규정된 상황에서, 적절한 안전조치를 제공하는 지 여부에 대한 의견을 제시한다.

8. 제7항에 명시된 견해는 해당 강령초안이나 개정 또는 확대 강령이 본 규정을 준수한다고 확정하거나 제3항에 규정된 상황에서, 적절한 안전조치를 제공한다고 확정하는 경우, 유럽정보보호이사회는 본 의견을 집행위원회에 제출한다.

9. 집행위원회는 시행령을 통해 제8항에 따라 제출된 공인된 행동강령이나 개정 또는 확대 강령이 유럽연합 내 일반적인 효력을 가지고 있음을 결정할 수 있다. 이러한 시행령은 제93조 (2)항에 규정된 심사 절차에 따라 채택되어야 한다.

10. 집행위원회는 제9항에 따라 일반적 효력을 갖는다고 판단된 공인된 강령에 대해 적절한 홍보를 보장해야 한다.

11. 유럽정보보호이사회는 공인된 행동강령과 개정 또는 확대된 강령 일체를 등록부에 수집하고 적절한 수단을 통해 이를 공개한다.

제41조
공인된 행동강령의 모니터링

1. 제57조와 제58조에 따른 관련 감독기관의 업무와 권한을 침해하지 않으면서, 제40조에 따른 행동강령의 준수에 대한 모니터링은 행동강령의 주제와 관련하여 적절한 수준의 전문지식을 보유하고, 관련 감독기관이 모니터링 목적으로 인가한 기구에 의해 수행될 수 있다.

2. 제1항에 규정된 기구는 하기 각 호에 해당하는 경우에는 행동강령의 준수를 모니터링하기 위해 인가될 수 있다.

(a) 강령의 주제와 관련하여 해당 기구가 감독기관이 납득할 수 있는 독립성과 전문성을 입증하는 경우;

(b) 강령을 적용하는 관련 정보처리자 및 수탁처리자의 자격을 평가하고 관련 조문의 준수를 감시하고 강령의 시행을 정기적으로 검토할 수 있는 절차를 수립한 경

우;

(c) 강령 위반에 대한 민원과 정보처리자나 수탁처리자가 강령을 시행하였거나 시행하는 방식을 처리하고 정보주체와 대중에게 해당 절차와 구조를 투명하게 공개하기 위한 절차와 구조를 수립한 경우;

(d) 그 업무와 직무가 이해의 상충을 초래하지 않는다는 사실을 관련 감독기관이 납득할 만한 수준으로 입증하는 경우.

3. 관련 감독기관은 제63조에 규정된 일관성 메커니즘에 따라, 본 조문의 1항에 규정된 기구의 인가를 위한 기준 초안을 유럽정보보호이사회에 제출해야 한다.

4. 관련 감독기관의 업무와 권한 및 제VIII장의 조문을 침해하지 않고, 제1항에 규정된 기구는 정보처리자 또는 수탁처리자의 강령 정지나 배제를 비롯하여 정보처리자 또는 수탁처리자에 의해 강령의 위반이 발생하는 경우, 적절한 보호수단에 의거하여 적절한 조치를 취해야 한다. 해당 기구는 해당 조치와 해당 조치의 근거를 감독기관에 통지한다.

5. 인가 조건이 충족되지 않거나 해당 기구가 실시하는 조치가 규정에 위반한 경우, 감독기관은 제1항에 규정된 기구의 인가를 철회한다.

6. 본 조문은 공공기관 및 기구가 수행하는 처리에 적용되지 않는다.

제42조
인증

1. 회원국과 감독 기관, 유럽정보호이사회, 집행위원회는 정보처리자가 수행하는 처리작업이 본 규정을 준수하고 있음을 보여주기 위한 목적으로 특히 유럽연합의 차원의 개인정보보호 인증 매커니즘, 개인정보보호 인장 및 마크의 수립을 장려한다. 영세기업이나 중소기업의 구체적인 요구가 참작되어야 한다.

2. 본 규정에 적용 받는 정보처리자 또는 수탁처리자의 준수와 더불어, 제46조 (2)항의 (f)에 규정된 조건에 따라 제3조에 따라 본 규정에 적용 받지 않는 정보처리자 또는 수탁처리자가 제3국이나 국제기구로의 개인정보 이전에 대한 프레임워크 안에서 제공하는 적절한 안전조치의 존재를 입증하는 목적으로, 본 조문의 제5항에 따라 승인된 개인정보보호 인증 메커니즘이나 인장 또는 마크가 수립될 수 있다. 해당 정보처리자나 수탁처리자는 정보주체의 권리 등, 상기의 적절한 안전조치를 적용하기 위해 계약 증서 또는 기타의 법적 구속력이 있는 증서를 통해 구속력 및 강

제력(enforceable)있는 약정을 작성해야 한다.

3. 인증은 자발적이며 투명한 절차를 통해 제공되어야 한다.

4. 본 조문에 따른 인증은 정보처리자 또는 수탁처리자가 본 규정을 준수해야 한다는 책임을 경감하지 않으며, 제55조 또는 제56조에 따른 관련 감독기관의 업무와 권한을 침해하지 않는다.

5. 본 조문에 따른 인증은 제58조 (3)항에 따른 관련 감독기관이나 제63조에 따른 유럽정보보호이사회가 승인한 기준을 토대로, 해당 감독기관, 또는 제43조에 규정된 인증기구에 의해 발행될 수 있다. 해당 기준이 유럽정보보호이사회에 승인되는 경우, 이는 공용 인증인 유럽 정보 보호 인장(European Data Protection Seal)로 이어질 수 있다.

6. 인증 메커니즘에 처리를 제출한 정보처리자나 수탁처리자는 제 43조에 규정된 인증기구나, 가능한 경우, 관련 감독기관에, 인증 절차를 수행하는데 필요한 정보 및 처리 활동에 대한 접근 일체를 제공해야 한다.

7. 인증은 최대 3년간 정보처리자나 수탁처리자에게 발행되며 관련 요건이 충족되는 경우 동일한 조건에 따라 갱신할 수 있다. 제43조에 규정된 인증 기구, 또는 관련 감독기관은 인증 요건이 충족되지 않을 경우, 인증을 철회한다.

8. 유럽정보보호이사회는 인증 메커니즘과 개인정보보호 인장 및 마크의 일체를 등록부에 수집하고 적절한 수단을 통해 이를 공개한다.

제43조
인증 기구

1. 인증은 제57조 및 제58조에 따른 감독기관의 업무와 권한을 침해하지 않고 개인정보 보호와 관련하여 적절한 수준의 전문 지식을 보유한 인증 기구는 제58조 (2)항의 (h)에 따른 권한을 행사하는데 필요한 경우 감독 기관에 이를 통지한 후 인증을 발행 및 갱신한다. 각 회원국은 본 인증 기구가 다음 중 하나 또는 모든 기구로부터 인가되었는지 규정한다:

(a) 제55조나 제56조에 따른 감독기관;

(b) EN-ISO/IEC 17065/2012 및 제55조나 제56조에 따른 감독기관이 수립하는 추가 요건에 따라 유럽의회 및 이사회 규정 (EC) 765/2008에 따라 지명되는 국가 인가

기구.

2. 제1항에 규정된 인증기구는 다음 각 호에 경우에 한하여 제1항에 따라 인가될 수 있다.

(a) 인증 주제에 대해 감독기관이 납득할 수준으로 독립성과 전문지식을 입증한 경우;

(b) 제42조 (5)항에 규정되고 제55조 또는 제56조에 따른 관련 감독기관이 승인하거나, 제63조에 따라 유럽정보보호이사회가 승인한 기준을 준수하기 위한 경우;

(c) 개인정보 보호 인증과 인장, 마크의 발행과 정기 심사 및 철회에 대한 절차를 마련한 경우;

(d) 인증 위반에 관한 민원이나 정보처리자나 수탁처리자가 인증을 시행하였거나 시행하는 방식을 처리하기 위해, 또한 이러한 절차 및 구조를 정보주체 및 대중에게 투명하게 공개하기 위해 절자 및 구조를 수립한 경우; 또한,

(e) 해당 업무와 직무가 이해의 상충을 초래하지 않는다는 사실을 관할 감독기관이 납득할 만한 수준으로 입증하는 경우.

3. 제1항 및 제2항에 규정된 인증기구의 인가는 제55조나 제56조에 따른 관련 감독기관이나 제63조에 따른 유럽정보보호이사회가 승인한 기준에 근거하여 실시된다. 본 조문의 제1항의 (b)에 따른 인가의 경우, 본 요건은 규정(EC) 765/2008에서 예상되는 요건과 해당 인증기구의 방법과 절차를 기술하는 기술규칙을 보완한다.

4. 제1항에 규정된 인증 기구는 정보처리자나 수탁처리자의 본 규정 준수의 책임을 침해하지 않고 해당 인증이나 인증의 철회를 초래하는 적절한 평가에 대해 책임을 져야 한다. 인가는 최대 5년간 발행되며 동 기구가 본 규정의 요건을 충족하는 경우 동일한 조건으로 갱신될 수 있다.

5. 제1항에 규정된 인증 기구는 감독기관에 인증 요청의 교부나 철회의 사유를 제시한다.

6. 감독기관은 쉽게 접근할 수 있는 양식으로 제3항에 규정된 요건과 제42조 (5)항에 규정된 기준을 공개한다. 아울러 감독기관은 유럽정보보호이사회에 해당 요건과 기준을 전송한다. 유럽정보보호이사회는 인증 메커니즘과 정보 보호 인장 일체를 등록부에 수집하고 적절한 수단을 통해 이를 공개한다.

7. 인가 조건이 충족되지 않거나 더 이상 충족되지 않는 경우, 또는 인증기구가 실시한 조치가 본 규정을 위반하는 경우, 관련 감독기관이나 국가 인가 기구는 제VIII장의 규정을 침해하지 않고 제1항에 언급되는 인증 기구에 부여되는 인가를 철회한다.

8. 집행위원회는 제42조 (1)항에 규정된 개인정보보호 인증 메커니즘에 고려되어야 할 요건을 규정할 목적으로 제92조에 따라 위임 법률을 채택할 권한이 있다.

9. 집행위원회는 인증 메커니즘과 개인정보보호 인장과 마크에 대한 기술적 기준과 이러한 인증 메커니즘을 홍보하고 인정하는 메커니즘을 규정하는 시행법률을 채택할 수 있다. 해당 시행법률은 제93조 (2)항에 규정된 심사 절차에 따라 채택될 수 있다.

제V장
제3국 및 국제기구로의 개인정보 이전

제44조
이전을 위한 통칙

현재 처리 중이거나 제3국 또는 국제기구로의 이전 후에 처리될 예정인 개인정보는 본 규정의 나머지 조문에 따라 정보처리자와 수탁처리자가 본 장에 규정된 조건을 준수하는 경우에만 이전이 가능하다. 여기에는 해당 제3국이나 국제기구로부터 기타 제3국이나 국제기구로 개인정보가 이전되는 경우도 포함된다. 본 장의 규정 일체는 본 규정을 통해 보증되는 개인의 보호 수준을 보장하기 위해 적용된다.

제45조
적정성 결정에 따른 이전

1. 집행위원회가 제3국, 해당 제3국의 영토나 하나 이상의 지정 부문, 또는 국제기구가 적정한 보호수준을 보장한다고 결정한 경우 제3국 또는 국제기구로의 개인정보 이전이 가능하다. 이 경우 특별한 인가가 필요 없다.

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

법치주의, 인권 및 기본적 자유의 존중, 공안, 국방, 국가보안 및 형법, 공공기관의 개인정보 이용을 다룬 전반적·분야별 관련 법률, 이 같은 법률, 개인정보 규

칙, 전문성 규칙, 보안 조치의 시행(향후 기타 제3국 또는 국제기구로의 개인정보 이전을 위한 규칙도 포함. 이 규칙은 해당 제3국 또는 국제기구에서 준수되는 것임), 사법적 판례, 유효하고 구속력 있는 정보주체의 권리, 개인정보를 침해 당한 정보주체를 위한 유효한 행정적·사법적 구제책

정보주체의 권리 행사의 지원과 권고 및 회원국 감독기관들과의 협력 등 개인정보 보호 규정의 준수를 보장하고 강요할 의무가 있는, 제3국에 소재하거나 국제기구에 적용되는 하나 이상의 독립적 감독기관의 유무 및 해당 기관의 효과적인 작동 여부

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. 집행위원회는 보호 수준의 적정성 여부를 평가한 후 제3국, 해당 제3국의 영토나 하나 이상의 지정 부문, 또는 해당 국제기구가 본 조문 2호의 의미 내에서 적정한 보호 수준을 보장하는지를 판단할 수 있다. 시행법률은 최소한 4년마다의 정기적 검토를 위한 메커니즘을 규정해야 하고 검토에는 제3국이나 국제기구 내의 관련 추이사항 일체가 고려되어야 한다. 시행법률은 영토·부문별 적용에 대한 규정을 명시하고, 적용이 가능한 경우 본 조문 2호(b)의 감독기관(들)에 대해 확인해야 한다. 시행법률은 제93(2)조에 명시된 검토 절차에 따라 채택되어야 한다.

4. 집행위원회는 본 조문의 3호에 준하여 채택된 결정 및 지침 95/46/EC 제25(6)조를 근거로 채택된 결정의 작동에 영향을 미칠 수 있는 제3국 및 국제기구 내의 추이사항을 지속적으로 모니터링 해야 한다.

5. 집행위원회는 가용 정보를 통해, 특히 3호에 명시된 검토 이후 제3국, 해당 제3국의 영토나 하나 이상의 지정 부문, 또는 국제기구가 2호에서 의미하는 적정한 보호 수준을 더 이상 보장하지 않는다고 판단될 경우, 필요한 정도까지 소급효 없이 3호에 명시된 결정을 철회, 수정, 또는 중지시킬 수 있다. 시행법률은 제93(2)조에 명시된 검토 절차를 따라 채택되어야 한다.

충분히 타당하고 긴요한 시급성의 근거가 있는 경우, 제93(3)조의 절차에 따라 집행위원회는 즉시 적용 가능한 시행법률을 채택하여야 한다.

6. 집행위원회는 5호에 의거하여 내린 결정을 야기한 상황을 시정할 목적으로 제3국이나 국제기구와 협의에 들어가야 한다.

7. 5호에 의거한 결정은 제46-49조에 따른 해당의 제3국, 제3국의 영토나 하나 이상

의 지정 부문, 또는 국제기구로의 개인정보 이전을 침해하지 않는다.

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. 지침 95/46/EC, 제25조(6)를 근거로 집행위원회가 채택하는 결정은 본 조문의 3호나 5호에 따라 채택되는 집행위원회 결정으로 수정, 대체, 폐지될 때까지 유효해야 한다.

제46조
적절한 안전조치에 의한 이전

1. 제45조(3)에 의거한 결정이 없을 경우, 정보처리자나 수탁처리자는 적절한 안전조치를 제공한 경우에 한하여, 정보주체가 행사할 수 있는 권리와 유효한 법적 구제책이 제공되는 조건으로 제3국 또는 국제기구에 개인정보를 이전할 수 있다.

2. 1호의 적절한 안전조치는 감독기관의 특별한 인가를 요하지 아니하고 다음과 같이 제공될 수 있다:
(a) 공공기관 또는 기구 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) 정보주체의 권리 등 적절한 안전조치를 적용하기 위한 것으로 법적 구속력 및 강제력이 있는 제3국의 정보처리자나 수탁처리자의 의무가 수반되는 제40조에 의거한 공인 행동강령

(f) 정보주체의 권리 등 적절한 안전조치를 적용하기 위한 것으로 법적 구속력 및 강제력이 있는 제3국의 정보처리자나 수탁자처리자의 의무가 수반되는 제42조에 의거한 공인 인증 메커니즘

3. 1호의 적절한 안전조치는 관할 감독기관의 승인을 거쳐 다음을 통해서도 제공될 수 있다:

(a) 정보처리자나 수탁처리자와 제3국이나 국제기구의 정보처리자, 수탁처리자 또는 개인정보 수령인 간의 계약 조항

(b) 공공기관이나 기구 간의 행정 협정에 삽입될 것으로 강제력이 있고 유효한 정보주체의 권리를 포함한 규정

4. 감독기관은 본 조문의 3호에 명시된 사례의 경우 제63조의 일관성 메커니즘을 적용해야 한다.

5. 지침 95/46/EC의 제26조(2)를 근거로 회원국이나 감독기관이 부여하는 인가는 해당 감독기관이 필요한 경우 수정, 대체, 철회할 때까지 유효해야 한다. 지침 95/46/EC의 제26조(4)를 근거로 집행위원회가 채택하는 결정은 필요한 경우 본 조문의 2호에 따라 채택된 집행위원회 결정에 의해 수정, 대체 또는 철회될 때까지 유효해야 한다.

제47조
의무적 기업 규칙

1. 관할 감독기관은 제63조에 명시된 일관성 메커니즘에 따라 의무적 기업 규칙을 승인해야 한다. 단, 다음을 전제로 한다.

(a) 법적 구속력이 있으며 피고용인 등 공동 경제활동에 관여하는 사업체 집단 또는 기업 집단의 모든 구성원들에게 적용되고 그들에 의해 이행된다.

(b) 본인의 개인정보 처리와 관련하여 정보주체에게 명시적으로 구속력 있는 권리를 부여한다.

(c) 2호에 규정된 요건을 충족시킨다.

2. 1호에 명시된 의무적 기업 규칙은 최소한 다음을 명시해야 한다.

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

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

(c) 내외부적으로 법적 구속력이 있는 특성

(d) 목적제한과 데이터 최소화, 보관기간 제한, 정보 품질, 설계 및 기본설정에 의한 정보보호, 정보처리의 법적 근거, 특별한 유형의 개인정보 처리, 정보 보안 확보 대책 등의 일반 정보보호 원칙 및 향후 의무적 기업 규칙의 구속을 받지 않는 기구에 대한 정보이전과 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 의무적 기업 규칙 위반에 따른 구제 및 적절한 경우 보상을 받을 권리가 포함된 개인정보 처리에 관한 정보주체의 권리 및 이 권리를 행사하기 위한 수단

(f) 유럽연합에서 정하지 않은 관련 회원국의 의무적 기업 규칙 위반에 대한 정보처리자나 수탁처리자의 책임 인정. 정보처리자나 수탁처리자는 해당 회원국이 피해를 유발한 사건에 대하여 책임이 없음을 증명할 경우에 한해 책임의 전부 또는 일부를 면할 수 있다.

(g) 제13조 및 제14조에 더하여, 본 호의 (d), (e), (f)에 명시된 규정 등 의무적 기업 규칙에 관한 정보가 정보주체에 제공되는 방식

(h) 제37조에 의거하여 지정된 개인정보담당관 또는 교육 및 민원처리 감독을 비롯하여 집단 내에서 의무적 기업 규칙의 준수 여부를 감독하는 담당자 또는 주체의 업무

(i) 민원 절차

(j) 공동 경제활동에 관여하는 사업체 집단 또는 기업 집단 내의 의무적 기업 규칙의 준수 여부를 검증하기 위한 메커니즘. 이 같은 메커니즘은 정보보호 감사 및 정보주체의 권리 보호를 위한 시정조치를 보장할 방법을 포함해야 한다. 해당 검증 결과는 (h)에 언급된 개인이나 개체 및 기업 집단이나 그 사업을 총괄하는 이사회에게 전달해야 하고, 관할 감독기관의 요구가 있을 시 제공되어야 한다.

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

(l) 특히 (j)에서 언급한 조치의 검증 결과를 감독기관에 보고함으로써 확보할 수 있는, 사업체 집단 구성원의 규칙의 준수를 보장하기 위한 감독기관과의 협력 메커니즘

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

(n) 상시적 또는 정기적으로 개인정보를 열람(access)할 수 있는 인력을 대상으로 한 적절한 정보보호 교육.

3. 집행위원회는 본 조의 의미 내에서 의무적 기업 규칙에 대해 정보처리자, 수탁처리자, 감독기관 간에 이루어지는 정보 교환에 필요한 양식과 절차를 정할 수 있다. 이러한 시행법률은 제93조(3)에 명시된 검토 절차에 따라 채택되어야 한다.

제48조
유럽연합 법률로 인가되지 않은 정보의 이전 또는 공개

정보처리자나 수탁처리자가 개인정보를 이전하거나 공개하도록 요구하는 제3국의 법원·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.

제49조
특정 상황을 고려한 적용의 일부 제외

1. 제45조 3호의 적정성 결정이 없거나 제46조의 의무적 기업 규칙 등 적절한 안전조치가 없을 경우, 제3국이나 국제기구로의 개인정보 이전은 다음의 조건 하에서만 가능하다:

(a) 적정성 결정 및 적절한 안전조치가 없음으로 인해 정보주체에 발생할 수 있는 정보이전에 대한 위험을 고지 받은 후 정보주체가 명시적으로 이전에 동의한 경우.

(b) 정보주체와 정보처리자 간의 계약 이행을 위해 또는 정보주체의 요청에 의해 취해진 계약 전 사전 조치의 이행을 위해 정보이전을 해야 하는 경우.

(c) 정보주체의 이익을 위해 정보처리자와 기타의 개인이나 법인 간에 체결된 계약의 이행을 위해 정보이전을 해야 하는 경우.

(d) 중요한 공익상의 이유로 정보이전이 반드시 필요한 경우.

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

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

(g) 개인정보가 유럽연합 또는 회원국 법률에 따라 정보를 공개할 목적이거나 일반국민 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 규칙 등 제45조나 제46조의 조항을 토대로 할 수 없고, (a)-(g)에 따른 특정 상황에서의 일부 제외가 적용되지 않는 경우, 정보이전이 간헐적이고 한정된 숫자의 정보주체에만 적용되고 정보주체의 이익이나 권리 및 자유가 우선하지 않는 한 정보처리자가 추구하는 정당한 이익의 목적에 필요하며, 정보처리자가 정보이전과 관련한 일체의 정황을 평가한 후 그 결과를 토대로 개인정보 보호에 적절한 안전조치를 제시하는 경우에만 제3국이나 국제기구로의 정보이전이 가능하다. 정보처리자는 정보이전 사실을 감독기관에 고지해야 한다. 제13조 및 제14조에 명시된 정보에 덧붙여, 정보처리자는 해당 이전 사실 및 정보처리자가 추구하는 설득력 있는 정당한 이익에 관한 정보를 정보주체에 고지해야 한다.

2. 1호의 (g)에 따른 정보이전은 개인정보 기록부에 포함된 개인정보의 전부 또는 전체 범주와 관련되어서는 아니 된다. 개인정보 기록부가 정당한 이익을 갖고 있는 사람을 위한 참조(조회)의 목적으로 만들어진 경우, 정보의 이전은 이 사람들이 요청하는 경우 또는 이들이 수령인인 경우에만 가능하다.

3. 1호 첫 단락의 (a), (b), (c) 및 두 번째 단락은 공공기관이 공권력을 집행하는 과정에서 시행하는 업무에는 적용되어서는 아니 된다.

4. 1호의 (d)에 언급된 공익은 정보처리자가 적용을 받는 유럽연합 또는 회원국 법률에서 반드시 인정되어야 한다.

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. 정보처리자나 수탁처리자는 제30조에 언급된 기록부(records)에 1호의 두 번째 단락에 명시된 평가 및 적절한 안전조치를 문서화해야 한다.

제50조
개인정보 보호를 위한 국제협력

집행위원회와 감독기관은 제3국 및 국제기구와 관련하여 다음의 사항을 적절히 이행하여야 한다.

(a) 개인정보 보호를 위한 법률을 효과적으로 집행하기 위한 국제협력 메커니즘 개발

(b) 개인정보와 기타 기본권 및 자유의 보호를 위한 적절한 안전조치를 조건으로, 통지, 민원 이첩, 조사 지원, 정보 교환 등을 통해 개인정보 보호를 위한 법률 집행에 대하여 국제 상호지원 제공

(c) 개인정보 보호를 위한 법률 집행 과정에서 국제협력을 촉진시킬 목적으로 논의 및 활동에 이해 당사자들을 참여시킬 것

(d) 제3국과의 사법 분쟁 등 개인정보 보호 법률 및 관행에 대한 교류 및 문서화를 촉진

제VI장
독립적인 감독기관

제1절
독립적인 지위

제51조
감독기관

1. 각 회원국은 처리와 관련하여 개인의 기본권과 자유를 보호하고 유럽연합 역내에서 개인 정보의 자유로운 이동을 촉진하기 위하여, 본 규정의 적용에 대한 모니터링을 전담할 하나 이상의 독립적인 공공기관을 제공해야 한다.

2. 각 감독기관은 유럽 연합 전역에 걸친 본 규정의 일관적인 적용에 일조해야 한다. 감독기관은 이러한 목적으로 제VII장에 의거하여 상호 간에 협력하고 집행위원회와 공조해야 한다.

3. 하나의 회원국에서 복수의 감독기관이 만들어질 경우, 해당 회원국은 유럽정보보

호이사회에서 해당 감독기관들을 대표할 감독기관을 지정하고 제63조에 규정된 일관성 메커니즘과 관련한 규정을 다른 기관이 준수하도록 보장하는 메커니즘을 수립해야 한다.

4. 각 회원국은 제 VI장에 의거하여 채택한 자국 법률의 조항을 최소한 [본 규정의 발효일자로부터 2년까지] 집행위원회에 고지하며, 이에 영향을 미치는 후속 개정안은 지체 없이 고지해야 한다.

제52조
독립성

1. 각 감독기관은 본 규정에 따른 직무를 수행하고 권한을 행사하는 과정에서 완전한 독립성을 가지고 활동해야 한다.

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. 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. 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. 각 회원국은 각 감독기관이 본 감독기관의 구성원의 지시만을 따르는 자체 인력을 선정 및 보유하도록 보장해야 한다.

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.

제53조
감독기관 위원(들)의 일반 조건

1. 회원국은 감독기관의 각 위원이 아래 각 호의 투명한 절차를 통해 임명되도록 해야 한다.
- 의회;

- 정부;
- 국가 수장;
- 회원국 법률에 의해 임명이 위임된 독립적 기구.

2. 각 위원은 특히 개인정보 보호 분야에서, 각자의 직무를 수행하고 권한을 행사하는 데 필요한 자격과 경험 및 기량을 갖춰야 한다.

3. 해당 회원국의 법률에 의거한 임기 만료, 사임, 또는 강제 해임 시 위원의 직무는 종료된다.

4. 위원은 중대한 위법행위가 있거나 직무 수행에 요구되는 조건을 더 이상 충족시키지 못하는 경우, 해임되어야 한다.

제54조
감독기관 설립 규칙(Rules)

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) 본규제의발효후첫임명을제외하고, 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 감독 기관 위원(들)의 재임명 가능여부 및 임기 연장의 횟수;

(f) 각 감독기관의 임직원의 의무에 관한 조건, 임기 도중과 이후 그에 저촉되는(incompatible) 행위나 직업, 편익에 대한 금지, 고용 중단에 관한 규칙.

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.

제2절

법적 자격, 업무 및 권한

제55조
법적 자격(competence)

1. 각 감독기관은 본 규제에 의거하여 자체 회원국 영토에서 부여된 임무를 수행하고 권한을 행사하기 위한 법적 자격을 지닌다.

2. 제6조 (1)항의 (c) 또는 (e)를 근거로 활동하는 공공기관이나 민간기구에 의해 처리가 수행되는 경우, 해당 회원국의 감독기관은 이에 대한 법적 자격을 갖는다. 이 경우 제56조는 적용되지 아니한다.

3. 감독기관은 사법능력을 행사하는 법원의 처리방식을 감독할 법적 자격은 없다.

제56조
선임 감독기관의 법적 자격

1. 정보처리자 또는 수탁처리자의 주 사업장이나 단일의 사업장의 감독기구는, 제55조를 침해하지 않으며, 제60조에 규정된 절차에 따라 정보처리자 또는 수탁처리자가 수행하는 회원국 간의 처리에 대해 선임 감독기관으로 행동할 법적 자격을 지닌다.

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 정보주체에만 중대한 영향을 미치는 경우에만 해당된다.

3. 본 조문의 제2항 규정된 상황의 경우, 해당 감독기관은 지체 없이 관련 사안에 대해 선임 감독기관에 통지해야 한다. 통지를 받은 후 3주 이내에, 선임 감독기관은 감독기관이 고지한 회원국의 정보처리자 또는 수탁처리자의 사업장의 존재 여부를 고려하여, 제60조에 규정된 절차에 따라, 해당 상황을 처리할 지 여부를 결정해야 한다.

4. 선임 감독기관이 관련 상황을 처리하기로 결정할 경우, 제60에 규정된 절차가 적용된다. 선임 감독기관에 통보한 감독기관은 선임 감독기관에 결정문의 초안을 제출한다. 선임 감독기관은 제60조 (3)항에 규정된 결정문 초안을 작성할 때, 해당 초안을 최대한 고려해야 한다.

5. 선임 감독기관이 관련 상황을 처리하지 않기로 결정할 경우, 선임 감독기관에 통보한 감독 기관은 제61조와 제62조에 의거하여 해당 상황을 처리해야 한다.

6. 선임 감독기관은 정보처리자나 수탁처리자가 수행하는 회원국 간의 처리에 대해 정보처리자 또는 수탁처리자의 유일한 교섭담당기관이다.

제57조
업무
1. 본 규정에 규정된 다른 업무에 영향을 미치지 아니하고, 각 감독기관은 담당 권역에서 다음을 수행한다.

(a) 본 규정의 적용에 대한 모니터링 및 집행;

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

(c) 회원국 법률, 국가 의회, 정부 및 다른 기관 및 기구에 따라, 처리와 관련한 개인의 권리 및 자유의 보호에 대한 법률 및 행정 조치에 대한 자문;

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

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

(f) 정보주체나 기구, 기관 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, 그러하다;

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

(h) 기타 감독기관이나 공공기관으로부터 수령 받은 정보 등을 근거로 본 규정의 적용에 대한 조사 실시;

(i) 특히 정보통신기술 및 상업적 관행의 개발 과정에서 개인정보 보호에 영향을 미치는 범위에서 관련전개(developments) 상황에대한모니터;

(j) 제28조의 (8)항과 제46조 (2)항의 (d)에 규정된 정보보호 표준계약조항(standard contractual clauses)의 채택;

(k) 제35조의 (4)항에 따라 개인정보보호 영향평가에 대한 요건과 관련한 목록을 수립 및 유지;

(l) 제36조 (2)항에 규정된 처리 작업에 관한 자문 제공;

(m) 제40조에 의거한 행동강령의 마련을 장려하고 의견을 제시하며, 제40조 (5)항에 따라 충분한 안전조치를 제공하는 행동강령을 승인;

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

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

(p) 제41조에 의거한 행동강령의 모니터링 기구 및 제43조에 의거한 인증 기구의 인가에 대한 기준의 초안 마련 및 공표;

(q) 제41조에 의거한 행동강령의 모니터링 기구의 및 제43조에 의거한 인증기관의 인가 시행;

(r) 제46조 (3)항에 규정된 계약조항 및 조문에 대한 승인;;

(s) 제47조에 의거한 의무적 기업규칙(biding corporate rules)에 대한 승인;

(t) 유럽정보보호이사회의 활동에 기여;

(u) 본 규정의 위반과 제58조 (2)항에 따라 취해지는 조치에 대한 내부적 기록 보관;

(v) 개인정보 보호와 관련된 기타 업무 수행;

2. 각 감독기관은 다른 통지 수단을 배제하지 않고, 전자 양식으로도 작성 가능한 민원 제출 양식 등의 조치로 제1항의 (f)에 규정된 민원의 제출을 용이하게 한다.

3. 각 감독기관의 업무의 수행에 대한 비용은 정보주체의 경우 무료이며, 해당되는

경우, 개인정보보호 담당관도 무료이다.

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.

제58조
권한

1. 각 감독 기관은 아래의 조사 권한을 모두 보유한다.

(a) 정보처리자와 수탁처리자 그리고 해당되는 경우, 정보처리자 또는 수탁처리자의 대리인에게 업무의 수행에 필요한 정보의 일체를 제공하도록 명령;

(b) 개인정보보호 감사의 형식의 조사 실시;

(c) 제42조 (7)항에 의거하여 발급된(issued) 인증에 대한 검토 실시;

(d) 정보처리자 또는 수탁처리자에게 본 규정의 위반 혐의 사안의 통지;

(e) 정보처리자 또는 수탁처리자로부터 업무의 수행에 필요한 모든 개인정보 및 모든 정보에 대한 열람권 취득;

(f) 유럽연합 또는 회원국의 절차 법률에 따라, 모든 개인정보 처리 장치 및 수단 등, 정보처리자와 수탁처리자의 영역에 대한 열람권 취득;

2. 각 감독기관은 다음의 시정 권한을 모두 보유한다.

(a) 예정된 처리작업(들)이 본 규정의 조문을 위반할 가능성이 높은 것에 대해 정보처리자 또는 수탁처리자에게 경고 발령;

(b) 예정된 처리작업(들)이 본 규정의 조문을 위반한 경우, 정보처리자 및 수탁처리자를 견책;

(c) 정보처리자 및 수탁처리자가 본 규정에 따라 본인의 권리를 행사하고자 하는 정보주체의 요청을 따를 것을 지시;

(d) 정보처리자 또는 수탁처리자에게 처리작업(들)이 본 규정의 조문을 준수하도록 지시하며, 적절한 경우, 구체적인 방식과 구체적인 기간 내에 하도록 지시;

(e) 정보주체에게 개인정보 유출에 대해 통지하도록 정보처리자에게 지시;

(f) 처리에 대한 금지 등, 임시 또는 확정적 제한의 부과;

(g) 제16조, 제17조, 제18조에 따른 처리의 수정이나 삭제 또는 제한을 지시하고, 제17조 (2)항 및 제19조에 따라 개인정보를 제공 받는 수령인들에게 이러한 행동조치에 대한 통지를 지시;

(h) 인증의 요건이 충족되지 않거나 더 이상 충족되지 않는 경우, 인증을 철회하거나 인증기구에게 제42조 및 제42조에 의거하여 발급된 인증을 철회하라고 지시하거나 인증기구에게 인증을 발급하지 않도록 지시;

(i) 각 개별 상황 별 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.

3. 각 감독 기관은 다음의 모든 인가 및 자문권한을 보유한다.

(a) 제36조에 규정된 사전 자문의 절차에 따라 정보처리자에게 자문을 제공;

(b) 자체 재량이나 요구에 따라, 해당 국가의 국회, 회원국의 정부 또는 회원국 법률에 따라 다른 기관 및 기구와 대중에게 개인정보보호와 관련한 사안에 대한 의견을 제공;

(c) 회원국 법률에서 사전 승인을 요구하는 경우, 제36조 (5)항에 규정된 처리에 대한 승인;

(d) 제40조 (5)항에 따른 의견 제공 또는 행동강령의 초안에 대한 승인;

(e) 제42조에 따른 인증기구의 인가;

(f) 제42조 (5)항에 따른 인증 발급 또는 인증의 기준에 대한 승인;

(g) 제28조 (8)항 및 제46조 (2)항에 규정된 정보보호 표준조항의 채택;

(h) 제46조 (3)항의 (a)에 규정된 정보보호 계약조항에 대한 승인;

(i) 제46조의 (3)항의 (b)에 규정된 행정적 협약에 대한 승인;

(j) 제47조에 따른 의무적 기업규칙에 대한 승인.

4. 본 조문에 따른 감독기관에게 수여된 권한의 행사는 헌장에 따른 유럽연합 및 회원국 법률에 규정된 유효한 사법구제 및 정밀 실사 등, 적절한 안전조치에 적용받는다.

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.

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.

제59조
활동 보고서

각 감독기관은 신고된 위반사건의 유형과 제58조 (2)항에 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.

제VII장
협력 및 일관성

제1절
협력

제60조
선임 감독기관과 기타 관련 감독기관 간 협력

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. 선임 감독기관은 제61조에 의거하여 언제든지 기타 관련 감독기관에게 상호지원을 요청할 수 있고, 특히 조사를 실시하거나 타 회원국에 설립된 정보처리자 또는 수탁처리자에 관한 조치의 이행을 모니터링 하기 위해 제62조에 따른 공동 작업을 시행할 수도 있다.

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.

4. 나머지 관련 감독기관이 본 조문의 3호에 따라 자문을 받은 후 4주의 기간 내에 결정(안)에 대하여 적정하고 타당한 반대 의사를 표명할 경우, 선임 감독기관은 그 같은 적정하고 타당한 반대 의견에 따르지 않거나 그것이 적정하고 타당하지 않다는 의견이 있을 경우, 제63조에서 규정된 일관성 메커니즘에 그 사안을 상정해야 한다.

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 4호에 명시된 절차의 적용을 받는다.

6. 어느 관련 감독기관도 4호 및 5호에 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. 선임 감독기관은 해당 결정을 채택하고 정보처리자 또는 수탁처리자의 주 사업장이나 단일 사업장에 고지해야 하며, 경우에 따라 나머지 관련 감독기관 및 유럽정보보호이사회(Board)에도 관련 사실과 근거의 개요 등 해당 결정을 통보해야 한다. 민원을 접수한 감독기관은 민원인에게 결정에 대해 통보해야 한다.

8. 7호 적용의 일부 제외로 인해 민원이 묵살 또는 거부되는 경우, 해당 민원을 접수한 감독기관은 결정을 채택하고 그 사실을 민원인과 해당 정보처리자에게 알려야 한다.

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 정보처리자와 관련한 조치에 관한 부분에 대해 결정을 채택하고, 자국 영토에 있는 정보처리자 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 정보처리자 또는 수탁처리자에 통보해야 한다.

10. 7호 및 9호에 따라 선임 감독기관의 결정을 고지 받은 후, 정보처리자 또는 수탁처리자는 유럽연합 내 모든 사업장의 활동 중에 시행되는 정보처리에 대하여 그 결정을 준수하기 위해 필요한 조치를 취해야 한다. 정보처리자 또는 수탁처리자는 결정을 준수하기 위해 취한 조치를 선임 감독기관에게 고지하고, 선임 감독기관은 나머지 관련 감독기관에게 통보해야 한다.

11. 예외적인 상황에서 관련 감독기관이 정보주체의 이익을 보호하기 위해 시급히 조치를 취해야 할 필요가 있다고 판단할 근거가 있을 경우, 제66조에 명시된 시급성의 절차가 적용된다.

12. 선임 감독기관 및 나머지 관련 감독기관은 본 조문에 따라 요구되는 정보를 표준화된 형식을 사용하여 전자적 수단에 의해 상호 제공해야 한다.

제61조
상호 지원

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. 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. 지원 요청에는 요청의 목적과 요청 사유 등의 필요한 정보가 포함되어야 한다. 교환되는 정보는 당초 요청된 목적으로만 사용되어야 한다.

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) 요청에 응할 경우 본 규정 또는 요청을 접수한 감독기관이 적용 받는 유럽연합 또는 회원국 법률에 위배될 경우.

5. 요청을 받은 감독기관은 경우에 따라 요청에 응하기 위해 취한 조치의 결과 또는 진행 상황을 통지해야 한다. 요청을 받은 감독기관은 4호에 따라 요청의 응대를 거부하는 사유를 제공해야 한다.

6. 규정에 따라, 요청을 받은 감독기관은 타 감독기관이 요구한 정보를 표준화된 형식을 사용하여 전자적 수단으로 제공해야 한다.

7. 요청을 받은 감독기관은 상호 지원 요청에 의거하여 그들이 취한 조치에 대해 비용을 청구해서는 아니 된다. 감독기관들은 예외적인 상황에서 상호 지원의 제공으로 야기되는 특정 지출에 대해 서로 보상하는 규정에 대해 합의할 수 있다.

8. 한 감독기관이 타 감독기관으로부터 요청을 접수한 후 한 달 이내에 5호에 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. 집행위원회는, 시행법률을 통해, 본 조문에 명시된 상호 지원을 위한 형식과 절차 및 6호에 명시된 표준 양식 등 감독기관들 간, 그리고 감독기관과 유럽정보보호이사회 간에 전자적 수단에 의한 정보 교환 방식을 규정할 수 있다. 이 같은 시행법률은 제93조(2)에 명시된 검토절차에 따라 채택되어야 한다.

제62조
감독기관의 공동 작업

1. 감독기관은 적정한 경우 기타 회원국의 감독기관들이 관여하는 공동 조사 및 공동 이행 조치 등의 공동 작업을 수행해야 한다.

2. 정보처리자나 수탁처리자가 여러 회원국에 사업장을 두고 있거나 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 공

동 작업에 참여시키고 감독기관의 참여 요청에 지체 없이 응답하여야 한다.

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. 1호에 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. 자국 영토에서 피해가 초래된 회원국은 자체 직원이 초래한 피해에 적용 가능한 조건에 따라 피해를 보상해야 한다. 소속 직원이 타 회원국의 영토에서 타인에게 피해를 유발한 부속 감독기관의 회원국은 상대 회원국이 당사자에게 대신 지불한 피해액을 전액 변상해야 한다.

6. 제3자에 대한 권리 행사를 침해하지 않고 5호를 예외로 하여, 각 회원국은 1호에 규정된 사례의 경우 4호에 명시된 피해와 관련하여 타 회원국으로부터의 배상 요구를 자제해야 한다.

7. 공동 작업이 예정되어 있고 감독기관이 한 달 내에 2호의 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.

제2절
일관성

제63조
일관성 메커니즘

1. 유럽연합 전역에 본 규정을 일관되게 적용하기 위해, 감독기관들은 본 절에 명시된 일관성 메커니즘(consistency mechanism)을 통해 상호 간에, 그리고 적정한 경우 집행위원회와 협력해야 한다.

제64조
유럽정보보호이사회 의견

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 영향 평가 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 인가 기준을 승인하고자 할 경우

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

(e) 제46조(3)(a)에 명시된 계약 조항을 승인하고자 할 경우

(f) 제47조에 규정된 의무적 기업 규칙을 승인하고자 할 경우

2. 특히 관할 감독기관이 제61조에 따른 상호 지원의 의무나 제62조에 따른 공동작업의 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. 1호 및 2호에 명시된 사례의 경우, 유럽정보보호이사회는 동일 사안에 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. 1호에 명시되고 5호에 따라 이사회 소속 위원에게 회람되는 결정(안)에 대해 의장이 적시한 적정 기간 내에 반대하지 않는 위원은 결정(안)에 동의한 것으로 간주한다.

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. 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) 1호 및 2호에 명시된 해당 감독기관과 집행위원회에 의견서 통지 및 일반 공개

6. 3호에 명시된 기간 내에 관할 감독기관은 1호에 명시된 결정(안)을 채택해서는 아니 된다.

7. 1호에 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. 관련 감독기관이 7호에 명시된 기간 내에 유럽정보보호이사회 의장에게 이사회 의견의 전부 또는 일부를 따르지 않겠다는 의사를 적정한 근거와 함께 통보하는 경우, 제65조(1)이 적용되어야 한다.

제65조
유럽정보보호이사회의 분쟁 해결

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. 1호에 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. 1호에 명시된 결정은 타당하고 선임 감독기관과 모든 관련 감독기관을 대상으로 해야 하며 이들에게 구속력을 가져야 한다.

3. 유럽정보보호이사회는 2호에 명시된 기간 내에 결정문을 채택할 수 없었던 경우, 2호에 명시된 두 번째 달의 만료 후 2주 이내에 위원회 단순 다수결로 결정문을 채택해야 한다. 이사회 위원들이 분열될 경우, 의장의 의결로 결정문을 채택해야 한다.

4. 관련 감독기관은 2호 및 3호에 명시된 기간 동안 1호에 따라 유럽정보보호이사회에 제출된 사안에 대하여 결정을 채택해서는 아니 된다.

5. 유럽정보보호이사회 의장은 1호에 명시된 결정을 부당한 지체 없이 관련 감독기관에게 통보해야 한다. 집행위원회에도 통보해야 한다. 감독기관이 6호에 명시된 최종 결정을 통보한 후 이는 지체 없이 유럽정보보호이사회 웹사이트에 게재되어야 한다.

6. 선임 감독기관 또는 경우에 따라 민원을 접수한 감독기관은 1호에 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 정보처리자나 수탁처리자 및 정보주체에 각각 최종 결정이 고지되는 날짜를 유럽정보보호이사회에 통보해야 한다. 관련 감독기관들의 최종 결정은 제60조(7), (8) 및 (9)의 조건으로 채택되어야 한다. 최종 결정은 1호에 명시된 결정을 지칭하며, 5호에 따라 유럽정보보호이사회 웹사이트에 1호의 결정이 게재될 것임을 명시해야 한다. 최종 결정에는 1호에 명시된 결정이 첨부되어야 한다.

제66조
긴급성(시급성) 절차

예외적인 상황에서 관련 감독기관이 정보주체의 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 기간

을 지정하여 즉시 채택할 수 있다. 감독기관은 지체 없이 해당 조치 및 조치의 채택 사유를 나머지 감독기관, 유럽정보보호이사회 및 집행위원회에 전달해야 한다.

2. 감독기관이 1호에 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. 관할 감독기관이 정보주체의 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. 제64조(3) 및 제65조(2)의 적용을 일부 제외하여, 본 조문의 2호 및 3호에 명시된 긴급한 의견이나 법적 구속력이 있는 결정은 2주 이내에 이사회 위원들의 단순 다수결로 채택되어야 한다.

제67조
정보의 교환

1. 집행위원회는 감독기관들 간, 그리고 감독기관과 유럽정보보호이사회 간에 제64조에 명시된 표준화된 양식 등 전자적 수단으로 정보를 교환하기 위한 방식을 규정하기 위해 일반적 범위의 시행법률을 채택할 수 있다.

그 같은 시행법률은 제93조(2)에 명시된 검토절차에 따라 채택되어야 한다.

제3절
유럽정보보호이사회

제68조
유럽정보보호이사회

1. 유럽정보보호이사회(이사회)를 유럽연합 기구로 정하고 법인격을 가지도록 한다.

2. 이사회는 의장이 대표한다.

3. 이사회는 각 회원국 감독기관의 장과 유럽정보보호감독기구(European Data Protection Supervisor), 또는 각 대리인으로 구성된다.

4. 한 회원국에서 하나 이상의 감독기관이 본 규정에 따른 조문의 적용을 모니터링할 책임이 있는 경우, 해당 회원국의 법률에 따라 공동 대리인이 임명되어야 한다.

5. 집행위원회는 의결권 없이 이사회의 활동 및 회의에 참석할 권리가 있다. 집행위원회는 대리인을 지정해야 한다. 이사회 의장은 집행위원회에 이사회 활동을 통보해야 한다.

6. 제65조에 명시된 사례의 경우, 유럽정보보호감독기구는 유럽연합 산하기관이나 기구, 사무소, 기관에 적용되고 사실상 본 규정에 상응하는 원칙 및 규정에 관한 결정에 대해서만 의결권을 갖는다.

제69조
독립성

1. 유럽정보보호이사회는 제70조 및 제71조에 따른 임무를 수행하거나 권한을 행사할 때 독립적으로 활동한다.

2. 제70조(1)(b) 및 제70조(2)에 명시된 집행위원회의 요청을 침해하지 아니하여, 유럽정보보호이사회는 임무를 수행하거나 권한을 행사하는 중에 다른 어느 누구로부터도 지시를 구하거나 그들의 지시를 따르지 아니한다.

제70조
유럽정보보호이사회의 업무

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 정보처리자, 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 호의 (e)에 부합하는 가이드라인, 권고사항 및 모범사례를 발행한다.

(g) 개인정보 침해를 규명하고 제33조(1) 및 (2)에 명시된 부당한 지체를 결정하기 위해서, 그리고 정보처리자 또는 수탁처리자가 개인정보 침해에 대해 고지해야 하는 특정 상황에 대하여 본 호의 (e)에 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 호의 (e)에 부합하는 가이드라인, 권고사항 및 모범사례를 발행한다.

(i) 정보처리자가 준수하는 의무적 기업 규칙과 수탁처리자가 준수하는 의무적 기업 규칙 및 제47조에 명시된 관련 정보주체의 개인정보 보호를 보장하기 위한 추가적 필요요건을 기반으로 개인정보 이전의 기준 및 요건을 추가로 명시하기 위해 본 호의 (e)에 부합하는 가이드라인, 권고사항 및 모범사례를 발행한다.

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

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

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

(m) 제54조(2)에 따라 개인이 본 규정의 침해를 신고하기 위한 보편적 절차 수립에 대해 본 호의 (e)에 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 인증 기구의 인가 및 정기 검토를 실시하고 제43조(6)에 따라 인가된 기구 및 제42조(7)에 따라 제3국에 설립된 공인 정보처리자 또는 수탁처리자의 공공기록부(public register)를 유지한다.

(p) 제42조에 따라 인증 기구의 인가를 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·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.

2. 집행위원회가 유럽정보보호이사회의 자문을 요청하는 경우, 사안의 시급성을 감안하여 시한을 명시할 수 있다.

3. 유럽정보보호이사회는 집행위원회와 제93조에 명시된 위원회(committee)에 이사회의 의견, 가이드라인, 권고사항 및 모범사례를 전달해야 한다.

4. 유럽정보보호이사회는 적절한 경우 이해당사자와 협의하고 적정한 기간 내에 의견을 개진할 기회를 제공해야 한다. 이사회는 제76조를 침해하지 않고 협의 절차의 결과를 공개해야 한다.

제71조
보고서

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. 연례 보고서에는 제70(1)조의 (l)에 명시된 가이드라인, 권고사항과 모범사례 및 제65조에 명시된 법적 구속력이 있는 결정의 실제 적용에 관한 검토가 포함되어야 한다.

제72조
절차

1. 유럽정보보호이사회는 본 규정에서 별도로 규정하지 않는 한 이사회 위원의 단순 다수결로 결정을 내린다.

2. 유럽정보보호이사회는 위원의 2/3 다수결로 자체적인 절차 규정을 채택하고 자체적인 운영 방식을 조직한다.

제73조
의장

1. 유럽정보보호이사회는 위원들 중에서 단순 다수결로 의장 1인과 부의장 2인을 선출한다.

2. 의장과 부의장의 임기는 5년으로 하고 1회 연임이 가능하다.

제74조
의장의 역할

1. 의장은 다음의 업무를 수행해야 한다:

(a) 유럽정보보호이사회 회의를 소집하고 안건을 준비한다.

(b) 제65조에 의거하여 유럽정보보호이사회가 채택한 결정을 선임 감독기관 및 관련 감독기관에 통보한다.

(b) 특히 제63조의 일관성 메커니즘과 관련해 유럽정보보호이사회의 업무가 적시에 수행되도록 한다.

2. 유럽정보보호이사회는 이사회의 절차 규정에 의장과 부의장 간의 업무 분장을 규정해야 한다.

제75조
사무국

1. 유럽정보보호이사회는 유럽정보보호감독기구가 제공하는 사무국을 둔다.

2. 사무국은 이사회 의장의 지시에 따라 독자적으로 업무를 수행한다.

3. 본 규정이 유럽정보보호이사회에 부여한 업무를 수행하는데 관여하는 유럽정보보호감독기구의 직원은 유럽정보보호감독기구에 부여된 업무의 수행에 관여하는 직원과 별도의 보고 체계를 따라야 한다.

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. 사무국은 유럽정보보호이사회에 분석적, 행정적, 로지스틱 관련 지원을 제공해야 한다.

6. 사무국은 특히 다음에 대한 책임이 있다:

(a) 유럽정보보호이사회의 일일 업무
(b) 유럽정보보호이사회 위원들, 의장 및 유럽집행위원회 간의 소통
(c) 기타 기구 및 대중과의 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

제76조
기밀성

1. 유럽정보보호이사회는 절차 규정에 규정된 바와 같이 필요하다고 판단하는 경우 이사회의 논의를 기밀로 해야 한다.

2. 유럽정보보호이사회 위원, 전문가 및 제3자의 대리인에게 제출된 문서의 열람(access)은 유럽의회 및 각료이사회 규정서 (EC) No 1049/2001의 규제를 받는다.

제VIII장
구제책, 책임, 처벌

제77조
감독기관에 민원을 제기할 권리

1. 다른 행정적 또는 법적 구제책을 침해하지 아니하여, 모든 정보주체는 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. 민원을 접수한 감독기관은 제78조에 의거한 법적 구제책의 가능성 등 민원 처리 경과 및 결과를 민원인에게 통보해야 한다.

제78조
감독기관에 대한 효과적인 사법구제권

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. 기타 행정적 또는 법적 구제책을 침해하지 아니하여, 각 정보주체는 제55조 및 제56조에 따른 관할 감독기관이 민원을 처리하지 않거나 3개월 이내에 정보주체에 제77조에 따라 접수된 민원의 처리 경과 또는 결과를 통보하지 않을 경우, 법적 구제책을 가질 권리가 있다.

3. 감독기관을 상대로 하는 법적 절차는 해당 감독기관이 설립된 회원국의 법정에서 진행된다.

4. 일관성 메커니즘에서 유럽정보보호이사회의 의견이나 결정에 이은 감독기관의 결정에 대하여 법적 절차가 제기될 경우, 감독기관은 그 의견이나 결정을 법원에 전달해야 한다.

제79조
정보처리자나 수탁처리자를 상대로 한 효과적인 사법구제권

1. 가용한 행정적 또는 제77조에 따른 감독기관에 민원을 제기할 권리 등 법률외적 구제책을 침해하지 아니하여, 각 정보주체는 본인에 관한 개인정보의 처리가 본 규정을 준수하지 않음으로 인해 본 규정에 의거한 본인의 권리가 침해되었다고 판단될 경우 사법적 구제책을 가질 권리가 있다.

2. 정보처리자 또는 수탁처리자를 상대로 한 법적 절차는 해당 정보처리자 또는 수탁처리자의 사업장이 있는 회원국의 법정에서 진행되어야 한다. 그렇지 않으면 정보처리자나 수탁처리자가 공적 권한을 행사하는 회원국의 공공기관이 아닌 한 정보주체의 거주지가 있는 회원국의 법정에서 절차가 진행될 수도 있다.

제80조

정보주체의 대리

1. 정보주체는 회원국 법률에 따라 적절히 구성되고 법정 목표가 공익에 있으며 개인정보 보호에 관한 정보주체의 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. 회원국은 개인정보 처리의 결과로 본 규정에 의거한 정보주체의 권리가 침해되었다고 판단될 경우, 1호에 명시된 기구, 조직 또는 협회가 정보주체의 권한에 관계없이 자국에서 제77조에 따른 관할 감독기관에 민원을 제기할 권리를 가진다고 규정할 수 있다.

제81조
법적 절차 중지

1. 회원국의 관할 법원이 타 회원국의 법원에 계류 중인 동일한 정보처리자나 수탁처리자의 정보처리에 대하여 동일한 사안의 법적 절차에 관한 정보를 가지고 있는 경우, 그 회원국의 법원에 연락하여 해당 법적 절차의 존재 유무를 확인해야 한다.

2. 동일 정보처리자나 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. 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.

제82조
보상 권리 및 책임

1. 본 규정의 침해로 인해 물질적 또는 비 물질적 피해를 입은 자는 누구든지 정보처리자 또는 수탁처리자로부터 피해 보상을 받을 권리가 있다.

2. 정보처리에 관여하는 정보처리자는 본 규정을 침해하는 정보처리로 초래된 피해에 대하여 책임을 져야 한다. 수탁처리자는 수탁처리자들에게 구체적으로 지시된 본 규정의 의무사항을 준수하지 않은 경우 또는 정보처리자의 합법적 지시를 벗어나거나 그 지시에 반대되는 행동을 한 경우에 한하여 정보처리로 초래된 피해에 대

하여 책임을 져야 한다.

3. 피해를 야기시킨 사건에 대하여 어떠한 식으로도 책임이 없음을 증명할 경우, 정보처리자 또는 수탁처리자는 2호에 의거한 책임에서 면제된다.

4. 하나 이상의 정보처리자 또는 수탁처리자가 동일한 정보처리에 관여하고 2호 및 3호에 따라 해당 정보처리로 초래된 피해에 대하여 책임이 있는 경우, 각 정보처리자나 수탁처리자는 정보주체의 유효한 보상을 보장하기 위해 피해 전체에 대하여 책임을 져야 한다.

5. 정보처리자 또는 수탁처리자가 4호에 따라 피해에 대해 전액 보상한 경우, 해당 정보처리자 또는 수탁처리자는 2호에 명시된 조건에 부합하여 동일한 정보처리에 관여한 기타 정보처리자나 수탁처리자에게 피해에 대한 그들의 책임 상응하는 보상액 일부를 청구할 수 있다.

6. 보상 받을 권리를 행사하기 위한 법정 절차는 제79조(2)에 명시된 회원국 법률에 따른 관할 법원에서 진행되어야 한다.

제83조
행정 과태료 부과에 관한 일반 조건

1. 각 감독기관은 4호, 5호 및 6호에 명시된 본 규정의 침해와 관련하여, 본 조문에 따른 행정 과태료의 부과가 개별 사례에서 유효하고 비례적이며 (침해행위를 하지 않도록 하는) 설득력이 있도록 해야 한다.

2. 행정 과태료는 각 개별 사례의 정황에 따라 제58조(2)의 (a)-(h) 및 (j)에 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 정보주체의 수와 피해 정도

(b) 고의적이거나 태만한 침해 특성

(c) 정보주체가 입은 피해를 완화하기 위해 정보처리자나 수탁처리자가 취한 조치

(d) 제25조 및 제32조에 의거하여 정보처리자 또는 수탁처리자가 이행한 기술·관리

적 대책을 고려한 정보처리자 또는 수탁처리자의 책임의 정도

(e) 정보처리자 또는 수탁처리자의 이전의 관련 침해건

(f) 침해를 구제하고 침해의 악영향을 완화하기 위한 감독기관과의 협력 수준

(g) 침해로 영향을 받은 개인정보의 범주

(h) 정보처리자 또는 수탁처리자가 침해를 통보했는지 여부 및 그런 경우 통보의 정도 등 침해 사실이 감독기관에 알려지게 된 방식

(i) 동일한 사안에 대하여 관련 정보처리자나 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 완화 요인

3. 정보처리자나 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. 다음과 같은 조문의 침해는 2호에 따라 10 000 000 유로에 이르는 행정 과태료 또는 사업체의 경우 직전 회계연도의 연간 전세계 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 정보처리자 및 수탁처리자의 의무

(b) 제42조 및 제43조에 따른 인증 기구의 의무

(c) 제41조(4)에 따른 모니터링 기구의 의무

5. 다음과 같은 조문의 침해는 2호에 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) 제5, 6, 7조 및 제9조에 따른 동의 조건을 비롯한 정보처리의 기본 원칙

(b) 제12-22조에 따른 정보주체의 권리

(c) 제44-49조에 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 열람(access)의 기회를 제공하지 않아 제58조(1)를 위반

6. 제58조(2)에 명시된 바와 같이 감독기관의 명령 불복은 2호에 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. 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. 본 조문에 따른 감독기관의 권한 행사는 유효한 사법 구제책 및 정당한 절차 등 유럽연합 또는 회원국 법률에 따라 적절한 절차상의 안전조치의 적용을 받는다.

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 호에 따라 채택하는 자국법의 조문을 집행위원회에 통보하고, 이에 영향을 미치는 차후의 개정법이나 개정안을 지체 없이 집행위원회에 통보해야 한다.

제84조
처벌

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. 각 회원국은 [본 규정의 발효일로부터 2년]까지 1호에 따라 채택하는 자국법의 조문을 집행위원회에 통보하고 이에 영향을 미치는 차후의 개정안을 지체 없이 집행위원회에 통보해야 한다.

제IX장
특정 정보처리 상황에 관한 규정

제85조
개인정보 처리 및 표현과 정보의 자유

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. 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(정보주체의 권리), 제4장(정보처리자 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. 각 회원국은 2호에 따라 채택한 자국법의 조문과 이에 영향을 미치는 차후의 개정법 또는 개정안을 지체 없이 집행위원회에 통보해야 한다.

제86조
개인정보 처리 및 공식 문서 공개

공공기관, 공공기구 또는 민간기구가 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 공공기관이나 기구에 적용되는 회원국 법률에 의거하여 해당 기관이나 기구가 공개할 수 있다.

제87조
국가 식별번호의 처리

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 정보주체의 권리 및 자유를 위한 적절한 안전조치가 있는 경우에 한해서만 활용되어야 한다.

제88조
고용 환경에서의 정보처리

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 의무이행 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. 그 같은 규정에는 특히 정보처리의 투명성과 공동 경제활동에 종사하는 사업체 또는 기업 집단 내에서 이루어지는 정보 이전, 직장에서의 모니터링 시스템과 관련하여 정보주체의 존엄성과 정당한 이익 및 기본권을 보호하는데 적절하고 구체적인 대책이 포함되어야 한다.

3. 각 회원국은 [본 규정의 발효일로부터 2년]까지 1호에 따라 채택하는 자국법의 조문을 집행위원회에 통보하고, 이에 영향을 미치는 차후의 개정안을 지체 없이 집행위원회에 통보해야 한다.

제89조
공익을 위한 유지보존의 목적, 과학이나 역사 연구의 목적 또는 통계 목적에서의 개인 정보 처리에 적용되는 안전조치 및 적용의 일부 제외

1. 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. 상기 목적들이 이 같은 방식으로 충족될 수 있다면 기술·관리적 조치에 가명처리가 포함될 수 있다. 정보주

체를 식별할 수 없거나 더 이상 식별할 수 없는 개인정보의 추가 처리를 통해 상기 목적들이 충족될 수 있는 경우, 그 목적들은 이 같은 방식으로 충족되어야 한다.

2. 개인정보가 과학이나 역사적 연구 목적 또는 통계 목적으로 처리되는 경우, 유럽연합 또는 회원국 법률은 제15, 16, 18조 및 제21조에 명시되고 본 조문 1호의 조건 및 안전조치에 따른 권리로 인해 특정 목적의 달성이 불가능하거나 심각하게 저해될 가능성이 있고 적용의 일부 제외가 그 같은 목적의 충족에 요구되는 한, 해당 권리의 적용을 일부 제외하도록 규정할 수 있다.

3. 공익을 위한 유지보존의 목적으로 개인정보가 처리되는 경우, 유럽연합 또는 회원국 법률은 제15, 16, 18, 19, 20조 및 제21조에 명시되고 본 조문 1호의 조건 및 안전조치에 따른 권리로 인해 특정 목적의 달성이 불가능하거나 심각하게 저해될 가능성이 있고 적용의 일부 제외가 그 같은 목적의 충족에 요구되는 한, 해당 권리의 적용을 일부 제외하도록 규정할 수 있다.

4. 2호 및 3호에 명시된 정보처리가 동시에 다른 목적으로 이루어지는 경우, 적용의 일부 제외는 해당 호에 명시된 목적을 가진 정보처리에만 적용되어야 한다. .

제90조
기밀유지의 의무

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 정보처리자나 수탁처리자와 관련하여 제58조(1)의 (e)와 (f)에 규정된 감독기관의 권한을 규정하는 특정 규정(rules)들을 채택할 수 있다. 이 같은 규정은 해당 기밀유지의 의무가 적용되는 활동의 결과로 또는 활동 중에 정보처리자나 수탁처리자가 입수한 개인정보에 한하여 적용되어야 한다.

2 각 회원국은 [본 규정의 발효일로부터 2년]까지 1호에 따라 채택하는 자국법의 조문을 집행위원회에 통보하고, 이에 영향을 미치는 차후의 개정안을 지체 없이 집행위원회에 통보해야 한다.

제91조
교회 및 종교 단체의 현행 정보보호 규정

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.

2. 1호에 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.

제X장
위임법률 및 시행법률

제92조
위임의 행사

1. 본 조문에 규정된 조건에 따라 집행위원회는 위임법률을 채택할 수 있는 권한을 부여 받는다.

2. 제12조(8) 및 제43조(8)에 명시된 권한의 위임은 본 규정의 발효일로부터 무기한으로 집행위원회에 부여된다.

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.  결정은유럽연합관보에게재된다음날또는거기에지정된차후의날짜에발효된다. 결정은 이미 발효 중인 위임법률의 유효성(효력)에는 영향을 미쳐서는 아니 된다.

4. 집행위원회는 위임법률의 채택 즉시 유럽의회와 각료이사회에 그 사실을 통보해야 한다.

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.

제93조
위원회(Committee) 절차

1. 집행위원회(Commission)는 위원회(committee)의 지원을 받아야 한다. 이 위원회는 규정서 (EU) No 182/2011의 범위에 해당하는 위원회이다.

2. 본 호를 참조하는 경우, 규정서 (EU) No 182/2011의 제5조가 적용되어야 한다.

3. 본 호를 참조하는 경우, 규정서 (EU) No 182/2011의 제5조 및 제8조가 적용되어야 한다.

제XI장
최종 규정

제94조
지침 95/46/EC의 폐기

1. 지침 95/46/EC는 [본 규정의 발효일로부터 2년]에 폐기된다.

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.

제95조
지침 2002/58/EC와의 관계

본 규정은 유럽연합 역내의 공공 통신분야에서 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.

제96조
이전에 체결된 협정과의 관계

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.

제97조
집행위원회 보고서

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. 1호에 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. 1호의 목적을 위하여, 집행위원회는 회원국과 감독기관에 정보를 요청할 수 있다.

4. 집행위원회는 1호 및 2호의 평가와 검토를 시행할 때 유럽의회, 각료이사회 및 기타 관련 기구나 정보원의 입장 및 조사결과를 참작해야 한다.

5. 집행위원회는 필요한 경우 특히 정보기술의 발전과 정보사회 발전 현황을 참작하여 본 규정을 개정하는데 적정한 제안서를 제출해야 한다.

제98조
기타 유럽연합의 정보보호 법률에 대한 검토

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 및 기관의 정보처리와 관련한 개인의 보호와 해당 개인정보의 자유로운 이동에 관한 규정에 관한 것이어야 한다.

제99조
발효 및 적용

1. 본 규정은 『유럽연합 관보(Official Journal of the European Union)』에 게재된 날로부터 20일 후에 발효된다.

2. 본 규정은 [본 규정의 발효 후 2년]부터 적용된다. *

본 규정은 전체로서 법적 구속력을 가지며 모든 회원국들에 직접적으로 적용 가능해야 한다.

유럽의회 의장

유럽각료이사회 의장

EU 개인정보보호법제(GDPR) 분석 및 개인정보보호법제 개선 입법past요 연구 2016. 7

개인정보보호위원회