개인정보의 처리와 관련한 개인의 보호 및 개인정보의 자유로운 이동에 관한 유럽의회와 유럽이사회 규정 (EU) No XXX/2016

해설전문번역

(1) 개인정보처리의 보호는 개인의 기본적인 권리이다. 유럽연합 기본권 헌장(이하 '헌장') 제8조(1)과 유럽연합 기능조약(이하 TFEU)의 제16(1)에서는 모든 사람은 본인의 개인정보를 보호할 권리가 있다고 규정하고 있다.

(2) 개인의 개인정보 처리 보호, 특히 개인정보 보호는 개개인의 국적 또는 거주지에 상관없이 개인의 기본적 권리와 자유로써 존중되어져야 함을 기본원칙으로 한다. 이 법은 자유, 안보 및 정의와 경제연합 분야의 성과, 경제 및 사회적 발전, 역내시장 경제의 강화 및 통합, 그리고 개인의 복지 증진을 목적으로 한다.

(3) 유럽의회 및 유럽 각료이사회의 지침 95/46/EC는 개인정보 처리 활동과 관련하여 개인의 기본적 권리 및 자유가 통일적으로 보호될 수 있도록 하며, 회원국 간에는 개인정보가 자유롭게 이동될 수 있도록 한다.

(4) 개인정보 처리는 인류에 기여할 수 있도록 설계되어야 한다. 개인정보 보호권은 절대적 권리가 아니며, 사회에서의 개인정보 보호 기능과 관련하여 고려되어야 하며 비례의 원칙에 입각하여 다른 기본권과 균형을 이루어야 한다. 본 규정은 모든 기본권을 존중하고, 여러 협약에서 구현되고 있는 헌장(Charter)의 자유와 원칙을 준수한다. 이러한 협약에는 특히 사생활 및 가족생활, 가정과 통신을 존중할 권리, 개인정보 보호, 사상과 양심 및 종교의 자유, 표현 및 정보의 자유, 기업 활동의 자유, 효과적인 구제 권리 및 공정한 재판을 받을 권리, 그리고 문화적·종교적·언어적 다양성 등이 포함된다.

(5) EU 내부시장 (기능) 활성화로 인한 경제적 및 사회적 통합은 회원국 간 개인정보 교류를 실질적으로 증가시켰다. 유럽연합 전역에서 개인, 단체 및 사업체 등 공공 및 민간 주체 사이의 개인정보 교류가 증가하고 있다. 회원국의 기관들은 유럽연합 법률에 따라 기관의 관련 임무를 이행하기 위한 목적이나, 또 다른 회원국의 기관을 위하여 임무를 수행하기 위한 목적으로 협력하고 개인정보를 교류해야 할 것을 요청받고 있다.

(6) 급격한 기술발전과 세계화에 따라 개인정보 보호 분야에 새로운 도전이 제기되었다. 개인정보의 수집 및 공유 규모가 상당한 수준으로 확대되었다. 기술을 통해 민간기업과 공공기관이 업무수행을 위해 전례 없는 규모로 개인정보를 활용하게 되었다. 개인들은 점점 더 많이 개인정보를 공개적으로, 그리고 세계적으로 활용될 수 있도록 하고 있다. 기술은 경제 및 사회생활을 변화시켜왔다. 앞으로는 기술을 통해 개인정보를 높은 수준으로 보호하는 한편, 유럽연합 역내에서, 그리고 제3국 및 국제기구로 개인정보가 자유로이 이동할 수 있도록 지원해야 한다.

(7) 역내 시장에서 디지털 경제를 발전시키기 위해서 신뢰 구축이 중요하다는 점을 고려하면, 강력한 집행력을 기반으로 하는 유럽연합에 더 강력하고 일관성 있는 개인정보 보호 프레임워크(framework)가 필요하다. 개인은 본인의 개인정보에 대한 통제권을 보유해야 한다. 개인, 경제주체 및 공공기관을 위한 법적, 실질적 확실성이 강화되어야 한다.

(8) 본 규정의 세부규정 및 제한사항을 각 회원국의 법률로써 규정하는 경우에는, 회원국은 일관성을 유지하고 회원국 법률의 수범자가 국가법률 규정을 이해하는 데 필요할 경우 자국법에 본 규정의 기본원칙(elements)을 편입할 수 있다.

(9) 지침 95/46/EC에 명시된 목적과 원칙이 여전히 타당한 한편, 해당 지침은 유럽 전역에서의 개인정보 보호와 관련한 일관성 결여, 법적 불확실성, 또는 특히 온라인 활동과 관련하여 개인을 보호하는 데는 중대한 위험이 있다는 광범위한 대중적 인식을 막지는 못하였다. 국가마다 개인정보 보호권 등 개인의 권리와 자유의 보호 수준이 상이함으로 인하여 유럽 전역의 자유로운 개인정보의 이동을 방해할 수 있다. 이러한 차이는 유럽연합 차원의 경제활동을 추구하는 데 장애물이 되거나, 경쟁을 왜곡하고 기관들이 유럽연합 법률에 따른 임무를 수행하는 것을 방해할 수 있다. 각 국의 보호 수준이 상이한 이유는 지침 95/46/EC의 집행 및 적용에 차이가 있었기 때문이다.

(10) 개인을 일관되게, 높은 수준으로 보호하고 역내 개인정보의 이동을 막는 장애물을 제거하기 위해서, 각 국은 개인정보 처리와 관련한 개인의 권리와 자유를 동일한 수준으로 보호해야 한다. 개인정보 처리와 관련한 개인의 기본권과 자유를 보호하기 위한 규정은 유럽 전역에 일관적이고 동일하게 적용되어야 한다. 공익을 위하거나 컨트롤러에 부여된 공적 권한에 따른 업무 수행에 있어 회원국은 본 규정을 적용함에 있어 한층 더 구체화하는 국내법 조문을 그대로 유지하거나, 신규 제정할 수 있다. 회원국은 지침 95/46/EC를 이행하는 개인정보 보호에 대한 일반적이며 수평적인 법률과 함께 좀 더 특정한 규정이 필요한 분야에 대해서는 특별법을 둔다. 또한 본 규정은 회원국에게 특별 범주의 개인정보('민감정보') 처리에 대해서 등 자체 규칙을 구체적으로 명시할 수 있는 운용의 여지를 제공한다. 이런 점에서, 본 규정은 개인정보 처리가 적법하다고 판단되는 조건에 대한 결정 등, 특정 처리 상황에 대한 정황을 규정하는 회원국의 법률을 배제하지 않는다.

(11) 유럽연합 전역에서 효율적으로 개인정보를 보호하기 위해 정보주체의 권리와 개인정보를 처리하고 그 처리를 결정하는 자의 의무를 강화하고 상세히 규정하는 것이 요구된다. 또한 회원국에서의 개인정보 보호 규칙의 준수를 모니터링하고 보장하기 위한 상응하는 권한 및 개인정보 침해에 대한 상응하는 제재도 요구된다.

(12) TFEU의 제16조(2)는 유럽의회와 각료이사회가 개인정보 처리에 관련된 개인을 보호하는 규칙 및 개인정보의 자유로운 이동에 관한 규칙을 정하도록 명하고 있다.

(13) 유럽연합 내에서 개인의 보호수준을 일관적으로 보장하고 역내 시장에서 개인정보의 자유로운 이동을 저해하는 회원국 간 차이를 방지하기 위하여, 본 규정은 영세, 중소기업 등 경제인에게 법적 확실성 및 투명성을 제공하고, 회원국의 개인에게는 동일한 수준의 법적으로 집행 가능한 권리를 제공하며, 컨트롤러와 프로세서에게는 의무와 책임을 부여하여 여러

회원국의 감독기관 간 효율적인 협력을 비롯하여 모든 회원국에서 개인정보 처리에 대한 일관적인 모니터링 및 동등한 제재를 보장하여야 한다. 역내시장이 적절하게 작동하기 위해서는 개인정보 처리와 관련한 개인의 보호와 연관된 이유로 유럽연합 내 개인정보의 자유로운 이동이 제한되거나 금지되지 않아야 한다. 영세 및 중소기업의 특정 상황을 고려하여, 본 규정은 기록보존과 관련된 250명 미만의 기관에 대한 적용의 일부제외를 두고 있다. 또한 유럽연합 산하기관 및 기구, 그리고 회원국 및 그 감독기관은 본 규정을 적용할 때 영세 및 중소기업의 특정한 니즈(needs)를 고려하도록 장려된다. 영세 및 중소기업의 개념은 위원회 권고 2003/361/EC에 대한 부록 제2조에 따라야 한다.

(14) 본 규정이 정하는 개인정보 보호는 국적이나 거주지에 상관없이 개인정보 처리와 관련된 개인에게 적용되어야 한다. 본 규정은 법인의 명칭과 형태 및 법인의 연락처 등 법인, 특히 법인으로 설립된 사업체와 관련된 개인정보의 처리는 다루지 않는다.

(15) 법의 적용 우회(circumvention)로 인한 심각한 위험을 방지하기 위해서, 개인보호는 기술적으로 중립적이어야 하고, 사용되는 기법에 의존해서는 안 된다. 개인정보가 파일링시스템에 포함되거나 포함될 예정이라면 자동화 방식에 의한 개인정보 처리 및 수동 처리에 대해서도 개인의 보호가 이루어져야 한다. 특정 기준에 따라 구성되지 않은 개인정보의 파일 또는 파일세트, 그리고 그 커버 페이지는 본 규정의 적용범위에 해당하지 않는다.

(16) 본 규정은 기본권 및 자유보장에 관한 사안, 그리고 국가안보와 관련한 활동과 같은 유럽연합 법률 영역 밖의 활동과 연관된 개인정보의 자유로운 이동에는 적용되지 않는다. 본 규정은 회원국이 유럽연합 공동의 외교 및 안보정책과 관련한 활동 시에 이루어지는 개인정보 처리에는 적용되지 않는다.

(17) 유럽 의회와 유럽 각료이사회의 규정(EC) No 45/2001은 유럽연합의 기관, 기구, 사무소 및 에이전시가 처리하는 개인정보에 적용된다. 이러한 개인정보처리에 적용 가능한 규정(EC) No 45/2001 및 기타 유럽연합 법률은 본 규정의 원칙과 규정에 맞게 조정되어야 하며 본 규정에 따라 적용되어야 한다. 유럽연합에서 더 강력하고 일관된 개인정보보호 프레임워크를 제공하기 위해서는 본 규정을 채택한 후, 본 규정과 동시에 적용시키기 위해 규정(EC) No 45/2001을 필요한 만큼 개정하여야 한다.

(18) 본 규정은 순수한 개인 또는 가정 활동 중에 발생하는 것으로서 직업적 또는 상업적 활동과는 연관이 없는 개인에 의한 개인정보의 처리에는 적용되지 않는다. 개인 또는 가정 활동에는 서신왕래와 주소지 보유, 또는 소셜 네트워크 활동 및 이러한 활동의 맥락에서 이루어지는 온라인 활동 등이 포함될 수 있다. 그러나 본 규정은 그 같은 개인 또는 가정활동을 위한 개인정보의 처리 수단을 제공하는 컨트롤러나 프로세서에게는 적용된다.

(19) 공공안보에 대한 위협으로부터 보호와 예방, 개인정보의 자유로운 이전 등 범죄예방, 수사, 적발 또는 기소, 또는 형벌 집행의 목적으로 관할 당국이 개인정보를 처리하는 것과 관련한 개인의 보호는 유럽연합 특별법에서 다룬다. 따라서 본 규정은 상기 목적을 위한 처리 활동에는 적용되지 않는다. 그러나 본 규정에 따라 공공기관이 처리하는 개인정보는 상기 목적으로 사용될 때 좀 더 특정한 유럽연합 법률, 즉 유럽의회 및 유럽 각료이사회 지침

(EU) 2016/680의 규제를 받는다. 회원국은 지침 (EU) 2016/680.이 지칭하는 관할 당국에 공공안보 위협으로부터의 보호와 예방, 개인정보의 자유로운 이전 등 반드시 범죄 예방, 수사, 적발 또는 기소, 또는 형벌의 집행을 목적으로 할 필요가 없는 업무를 맡길 수 있고 그러한 기타 목적의 개인정보의 처리는 유럽연합 법률의 적용범위에 해당하는 한 본 규정의 범위에 해당한다.

본 규정의 범위에 해당하는 목적으로 관할 당국이 개인정보를 처리하는 것과 관련하여, 회원국은 본 규정의 규칙 적용에 맞추기 위하여 좀 더 특정한 조문을 유지하거나 신설할 수 있어야 한다. 그러한 조문을 통해 각 회원국의 헌법적, 조직적, 행정적 구조를 참작하여 관할 당국이 상기의 기타 목적으로 개인정보를 처리하는 것에 대한 특정 요건을 더 정확히 결정할 수 있다. 민간기관의 개인정보 처리가 본 규정의 범위에 해당할 때, 본 규정은 회원국이 특정 조건에 따라 법률로써 특정의 의무 및 권리를 제한할 수 있음을 규정해야 한다. 단, 그 같은 제한이 공공안보에 대한 위협으로부터의 보호와 예방, 개인정보의 자유로운 이전 등 범죄 예방, 수사, 적발 또는 기소, 또는 형벌의 집행을 포함한 특정의 중요한 이익을 보호하기 위해 민주사회에서 필요하고 적절한 조치가 될 때 그러하다. 예를 들어, 자금세탁 방지 또는 법의학연구 활동의 체계에서 관련이 있다.

(20) 본 규정이 특히 법원과 기타 사법기관의 활동에 적용되는 한편, 유럽연합 또는 회원국 법률은 법원과 기타 사법기관의 개인정보 처리와 관련한 처리 작업 및 처리 절차를 명시할 수 있다. 감독기관의 권한은 의사결정 등 법원이 소관 사법 업무를 수행함에 있어 사법부의 독립성을 수호하고자 사법권한을 행사할 때의 개인정보 처리에는 미치지 않는다. 그 같은 데이터 처리 작업의 감독을 회원국 사법제도 내의 특정 기관에 위임할 수 있어야 하며, 그 기관은 특히 본 규정의 규칙 준수를 보장하고, 사법부 구성원 간에 본 규정에 따른 의무에 대한 인식을 제고하며, 그 데이터 처리 작업과 관련한 민원을 처리해야 한다.

(21) 본 규정은 유럽의회 및 유럽 각료이사회의 지침 2000/31/EC의 적용을 침해해서는 안 되며, 특히 동 지침 제12조에서 제15조까지의 중개서비스 제공자의 손해배상 원칙(liability rules)의 적용을 침해해서는 안 된다. 동 지침은 회원국 간 정보사회서비스의 자유로운 이동을 보장하여 역내 시장의 적절한 작동에 기여하고자 한다.

(22) 유럽연합 역내의 컨트롤러 또는 프로세서의 사업장(establishment) 활동과 관련한 개인정보 처리는 본 규정에 따라야 하고, 그 처리 자체가 유럽연합 역내에서 발생하는지 여부는 상관없다. 사업장이라 함은 안정적인 방식을 통해 효과적이고 실제적인 활동을 행하는 것을 의미한다. 그 방식의 법적 형태는 법인격을 가진 지점 또는 자회사를 통한 것인지에 관계없이 그와 관련한 결정적인 요인이 아니다.

(23) 개인이 본 규정에 따른 보호를 받을 수 있도록 하기 위하여 유럽연합 역내에 설립되지 않은 컨트롤러 또는 프로세서가 유럽연합 역내에 있는 정보주체의 개인정보를 처리할 때 그 처리 활동이 비용 지불과 연계되는지 여부에 관계없이 해당 정보주체에게 재화 또는 서비스를 제공하는 것과 관련되는 경우 본 규정의 적용을 받아야 한다. 그 컨트롤러 또는 프로세서가 유럽연합 역내의 정보주체에게 재화 또는 서비스를 제공하는지 여부를 결정하기 위하여 그들이 유럽연합 역내 하나 이상의 회원국의 정보주체에게 서비스를 제공할 계획이 있음

이 분명한지 여부를 확인해야 한다. 단지 유럽연합 역내에서 컨트롤러, 프로세서 또는 중개인의 웹사이트에 접근할 수 있다거나 이메일 주소 또는 기타 연락처를 열람할 수 있다는 것, 또는 컨트롤러가 설립된 제3국에서 통용되는 언어가 사용되는 것만으로는 그 같은 의사를 확인하기에는 불충분하고, 하나 이상의 회원국에서 통용되는 언어나 통화를 사용하고 그 언어로 재화와 서비스를 주문할 수 있다거나 유럽연합 역내의 소비자나 이용자에 대해 언급하는 등의 요인은 컨트롤러가 유럽연합 내의 정보주체에게 재화나 서비스를 제공할 계획이 있음을 분명하게 해 줄 수 있다.

(24) 유럽연합 역내에 설립되지 않은 컨트롤러 또는 프로세서가, 유럽연합 역내에 있는 정보주체의 개인정보를 처리할 때 그 처리가 해당 컨트롤러 또는 프로세서가 역내에서 발생하는 정보주체의 행동을 모니터링 하는 것과 관련 있을 때 본 규정을 적용받아야 한다. 처리 활동이 정보주체의 행동을 감시하기 위한 것으로 간주될 수 있는지 여부를 결정하기 위해서는, 특히 개인에 관한 결정을 내리거나 개인의 선호, 행동 및 태도를 분석하거나 예측하기 위해 그 개인을 프로파일링 하는 등의 개인정보 처리기법을 추후에 사용할 수 있는 점을 포함, 개인이 인터넷상에서 추적이 되는지 여부가 확인되어야 한다.

(25) 회원국 법률이 국제공법으로 적용되는 경우, 본 규정은 회원국의 외교공관 또는 영사관 내의 컨트롤러 등 유럽연합 역외에 설립된 컨트롤러에게도 적용될 수 있다.

(26) 개인정보 보호 원칙은 식별된 또는 식별될 수 있는 개인에 관한 일체의 정보에 적용된다. 가명처리를 거친 개인정보는 추가 정보의 사용으로 개인에 연계될 수 있는 정보로서, 식별 가능한 개인에 관한 정보로 간주되어야 한다. 개인이 식별 가능한지를 판단함에 있어 선별(singling out) 등 그 개인을 직간접적으로 식별하기 위해 컨트롤러 또는 제3자가 합리적으로 사용할 것으로 예상되는 모든 수단이 고려되어야 한다. 그 수단이 개인을 식별하는 데 사용될 것이라 합리적으로 예상되는지 여부를 확인하기 위해서 식별에 소요되는 비용 및 시간 등의 모든 객관적 요인을 고려하고, 처리 시점에 가용한 기술 및 기술 발전사항을 고려하여야 한다. 따라서 개인정보 보호 원칙은 익명정보, 즉 식별되었거나 식별 가능한 개인에 관련되지 않은 정보 또는 정보주체가 식별 가능하지 않거나 더 이상 식별 가능하지 않은 방식으로 익명 처리된 개인정보에는 적용되지 않는다. 따라서 본 규정은 통계 목적 또는 연구 목적 등을 위한 익명정보의 처리에는 적용되지 않는다.

(27) 본 규정은 망자의 개인정보에 적용되지 않는다. 회원국은 망자의 개인정보 처리에 대한 규칙을 규정할 수 있다.

(28) 개인정보에 가명처리를 적용하는 것은 관련 정보주체에게 미치는 위험성을 줄이고 컨트롤러와 프로세서가 개인정보 보호의 의무를 충족시킬 수 있도록 지원한다. 본 규정에서 명시적으로 '가명처리'를 도입하는 것이 기타의 개인정보 보호의 조치를 배제시키려는 의도는 아니다(가명처리를 하더라도 기타의 개인정보 보호 조치를 적용할 필요도 있음).

(29) 개인정보 처리 시 가명처리 적용에 대한 인센티브를 부여하기 위해서는 가명처리 조치가 일반적 분석은 허용하되 동종의 컨트롤러 사업체 내에서 가능할 수 있어야 한다. 이 때 동종의 컨트롤러 사업체 내의 컨트롤러는 관련 처리에 대하여 본 규정이 이행되고 개인정보

를 특정 정보주체에 연결시키는 추가 정보를 별도 보관하도록 하는 기술적·관리적 조치를 취했어야 한다. 개인정보를 처리하는 컨트롤러는 동종의 컨트롤러 사업체 내의 인가받은 사람을 가리킨다.

(30) 개인은 본인이 사용하는 기기, 애플리케이션, 툴, 프로토콜을 통해 제공되는 인터넷 프로토콜 주소, 쿠키 식별자 또는 전파식별태그 등의 기타 식별자인 온라인 식별자와 연결될 수 있다. 이러한 정보는 개인에 대한 자취를 남길 수 있고, 특히 서버를 통해 수신되는 '고유 식별자(unique identifies)' 및 다른 정보와 결합되는 경우, 해당 개인에 대한 프로파일을 생성하고 이들을 식별하는 데 사용될 수 있다.

(31) 관세청 및 국세청, 금융조사 기관, 독립 행정기관, 또는 증권시장 규제 및 감독책임의 금융시장 기구 등, 공적 임무 수행을 위한 법적 의무에 따라 개인정보를 제공받는 공공기관은 유럽연합 또는 회원국 법률에 따라 공공이익을 위한 특정 문의업무를 처리하는 데 필요한 개인정보를 받은 경우, 수령인으로 간주되지 않는다. 공공기관의 정보 제공 요청은 항상 서면 형식을 갖추어야 하고 타당하고 간헐적이어야 한다. 그 요청은 파일링시스템 전체에 대한 것이 아니어야 하고 파일링시스템 간에 상호연결이 이루어지도록 해서도 안 된다. 상기 공공기관의 개인정보 처리는 처리 목적에 따라 적용 가능한 데이터 보호 규칙을 준수하여 이루어져야 한다.

(32) 동의는 전자적 방식 등 서면 진술 또는 구두 진술 등으로, 정보주체가 본인과 관련한 개인정보의 처리에 대해 자발적이고 구체적이며 동의 내용에 대해 인지하는 분명한 합의를 나타내는 명확하고 적극적인 행위로써 제공되어야 한다. 인터넷 웹사이트의 개인정보 처리 동의란 체크, 정보사회서비스에 대한 기술적 설정 선택 또는 본인의 개인정보 처리 수락을 의미하는 정보주체의 행동이나 기타 진술이 이에 포함된다. 따라서 침묵, 사전 자동 체크된 개인정보처리 동의나 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 안 된다.

(33) 과학적 연구 목적의 경우, 개인정보 수집 당시에 개인정보 처리 목적을 충분히 확인하기가 불가능할 때가 많다. 따라서 정보주체는 과학적 연구의 공인 윤리 기준에 부합된 경우, 특정 연구 분야에 대해 동의를 제공할 수 있다. 의도한 처리 목적이 허용하는 선에서 정보주체는 특정 연구 분야 혹은 연구 일부분에 국한하여 본인의 동의를 제공할 수 있어야 한다.

(34) 유전자 정보는 특히 염색체 분석, 데옥시리보핵산(DNA) 분석 또는 리보핵산(RNA)분석 등 개인에게서 채취한 생물학적 샘플의 분석 결과나 이에 상응하는 정보를 입수할 수 있는 기타 요소의 분석으로부터 얻은 개인의 선천적 또는 후천적 유전자 특성에 관한 개인정보로 정의되어야 한다.

(35) 건강 관련 개인정보에는 정보주체의 과거, 현재, 혹은 미래의 신체적 또는 정신적 건강상태와 관련한 정보를 드러내는 모든 정보주체의 건강상태에 속하는 데이터가 포함된다. 이

정보에는 유럽 의회와 각료이사회의 지침 2011/24/EU에 규정된 바와 같이 의료서비스를 등록하고 정보주체에 제공하는 과정에서 수집된 개인에 대한 정보도 포함된다. 건강 목적으로 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) 컨트롤러의 유럽연합 역내 주 사업장은 컨트롤러의 유럽연합 내 중앙행정 지점이어야 하지만, 개인정보 처리 목적 및 방식에 대한 결정을 유럽연합 내 다른 사업장에서 내리는 경우, 그 사업장이 주 사업장으로 간주되어야 한다. 컨트롤러의 유럽연합 내 주 사업장은 객관적인 기준에 따라 결정되어야 하며, 안정적인 방식을 통해 처리 목적 및 방식에 대한 주요 결정을 내리는 관리활동을 효과적이고 실제적으로 행하는 것을 의미한다. 그 기준은 개인정보의 처리가 해당 지역에서 이루어지는지 여부에 따라 달라지지 않는다. 개인정보 처리 또는 처리활동을 위한 기술적 수단 및 기술이 존재하고 이를 사용한다는 그 자체가 주 사업장이 되지 않으므로 이는 주 사업장을 결정하는 기준이 아니다. 프로세서의 주 사업장은 프로세서의 유럽연합 내 중앙행정 지점이거나, 유럽연합 역내에서 중앙 행정처리가 이루어지지 않는 경우에는 유럽연합 내 주요 처리 활동이 발생하는 장소가 주 사업장이다. 컨트롤러와 프로세서 모두와 관련되어 있는 경우, 선임 감독기관은 처리자의 주 사업장이 있는 회원국의 감독기관이어야 하고 프로세서의 감독기관은 관련 감독기관으로 간주되어야 하며, 이 감독기관은 본 규정이 정한 협력 절차에 참여해야 한다. 어느 경우든, 프로세서의 단일 또는 복수의 사업장이 소재한 회원국 또는 복수의 회원국의 감독기관들은, 결정문 초안이 처리자에 한하여 관련되어 있는 경우, 관련 감독기관으로 간주되지 않는다. 사업체 집단이 처리를 수행하는 경우, 통제 사업체의 주 사업장은 사업체 집단의 주 사업장로 간주되어야하며, 처리 목적과 수단을 다른 사업체가 결정하는 경우는 예외로 한다.

(37) 사업체 집단(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 보호를 받아야 한다. 특정한 보호는 특히 마케팅 또는 사용자 프로필이나 가성인격 생성의 목적으로 아동의 개인정보를 사용하는 경우와 아동에게 직접 제공되는 서비스의 이용 시 아동과 관련한 개인정보를 수집하는 경우에 적용되어야 한다. 아동에게 직접 제공되는 예방 서비스 또는 카운슬링의 경우에는 친권 보유자의 동의가 필수적이지 않다.

(39) 모든 개인정보의 처리는 합법적이고 공정해야 한다. 본인과 관련된 개인정보가 수집, 이용, 참조되거나 기타 방식으로 처리된다는 사실, 그리고 그 개인정보가 처리되거나 처리될 범위를 해당 개인에게 투명하게 알려야 한다. 이러한 투명성 원칙은 개인정보 처리와 관련

하여 행하는 정보 제공(information) 및 의사소통(communication) 일체가 용이하고 이해하기 쉬우며 명확하고 평이한 언어로 행해지도록 요구한다. 투명성 원칙은 정보주체에게 제공되는 컨트롤러의 신원과 처리 목적에 대한 정보 및 해당 개인에 대한 공정하고 투명한 처리를 보장하기 위한 추가 정보, 그리고 본인에 관해 처리 중인 개인정보를 확인하고 전달받을 수 있는 개인의 권리에 관련된다. 개인은 개인정보 처리와 관련한 위험성, 규칙, 안전징치와 권리 및 그 권리를 행사하는 방식에 대해서 인지할 수 있어야 한다. 특히 개인정보가 처리되는 특정한 목적은 명백하고 적법하여야 하고, 해당 개인정보의 수집 당시에 결정되어야 한다. 개인정보는 처리 목적에 적합하고, 관련되며 그에 필요한 정도로 제한되어야 한다. 이는 특히 개인정보의 보관기관이 최소한으로 제한되도록 요구한다. 개인정보는 처리 목적이 여타 수단에 의해서는 합리적으로 성취될 수 없는 경우에 한하여 처리 될 수 있다. 컨트롤러는 개인정보가 필요 이상으로 보관되지 않도록 기간을 정해 삭제 또는 주기적 검토가 이루어지도록 해야 한다. 모든 적정 조치를 취해 부정확한 개인정보가 수정 또는 삭제되도록 해야 한다. 개인정보는 개인정보 및 그 처리에 사용되는 장비에 무단으로 접근하거나 사용하는 것을 방지하는 등 적절한 안정과 기밀성을 보장하는 방식으로 처리되어야 한다.

(40) 처리가 합법적이기 위해서는 관련 정보주체의 동의를 근거로 하거나, 본 규정이나 본 규정에 명시된 유럽연합 또는 회원국 법률에 규정된 기타 적법한 근거를 기반으로 하여야 한다. 컨트롤러에게 부과된 법적 의무의 준수, 정보주체가 계약 당사자가 되는 계약의 이행 또는 계약 체결 전에 정보주체의 요청에 따른 조치 시행 등이 이에 해당한다.

(41) 본 규정이 법적 근거나 입법 조치를 규정하고 있는 경우, 그 규정들이 반드시 회원국 의회가 채택한 것일 필요는 없으나 회원국의 헌법적 질서에 따른 요건을 침해해서는 안 된다. 그러나 그 법적 근거 또는 법적 조치는 명확하고 정확해야 하고 이를 적용받는 개인이 유럽 사법재판소와 유럽 인권재판소의 판례법에 따라 그 적용을 예측할 수 있어야 한다.

(42) 처리가 정보주체의 동의에 근거하는 경우, 컨트롤러는 정보주체가 처리 방식에 대해 동의를 제공하였음을 입증할 수 있어야 한다. 특히 처리되는 사안이 아닌 다른 사안에 대해서면 진술로 동의하는 경우, 안전장치를 통해 정보주체가 동의가 제공되었다는 사실과 어느 범위까지 동의가 제공되는지에 대해 인지하도록 해야 한다. 유럽이사회 지침 93/13/EEC1에 따라, 컨트롤러가 사전에 작성한 동의 진술서는 명확하고 평이한 언어를 사용하여 이해할 수 있고 열람이 용이하여야 하며 불공정한 용어를 포함해서는 안 된다. 동의 내용을 인지한 동의가 되기 위해 정보주체는 최소한 컨트롤러의 신원과 예정된 개인정보 처리 목적에 대해 인지하고 있어야 한다. 정보주체가 진정으로 또는 자유 선택으로 동의하지 않았거나, 불이익 없이 동의를 거절하거나 철회할 수 없는 경우에는 해당 동의는 자유롭게 제공된 것이라고 간주되지 않는다.

(43) 동의가 자유롭게 제공되도록 하기 위해서는, 정보주체와 컨트롤러 간의 명백한 불균형이 존재하는 특정 상황과 같은 경우에는 동의가 유효한 법적 근거가 되지 않으며, 특히 컨트롤러가 공공기관임으로 인해 그 특정 상황의 모든 정황에서 동의가 자유롭게 제공되었을 것이라 예상되지 않는 경우에는 더욱 그러하다. 서로 다른 개인정보 처리 작업에 개별 동의를 제공하는 것이 개별 사례에서 적절함에도 불구하고 그렇게 할 수 없는 경우 또는 서비스 제공 등의 계약의 이행이 동의 없이 이루어질 수 있음에도 불구하고 동의에 근거하여 진행

되는 경우 동의는 자유롭게 제공된 것이 아니라고 간주된다.

(44) 개인정보 처리가 계약 자체 또는 계약을 체결하고자 할 경우 요구된다면 이는 적법하다.

(45) 컨트롤러에게 부과된 법적 의무에 따라 처리가 이루어지는 경우 또는 공익을 위하거나 공적 권한 행사에 따른 직무 수행에 개인정보 처리가 필요한 경우, 해당 처리는 유럽연합 또는 회원국 법률에 그 근거를 두어야 한다. 본 규정은 각 개별 처리에 대하여 특정 법률을 요구하지는 않는다. 컨트롤러에 적용되는 법적 의무에 근거한 복수의 처리작업 또는 공익을 위하거나 공적 권한 행사에 따른 직무 수행에 처리가 요구되는 경우에 대한 근거가 된다면 하나의 법으로도 충분할 수 있다. 유럽연합 또는 회원국 법률은 처리 목적도 결정하여야 한다. 또한 그 법률은 개인정보 처리의 적법성을 관장하는 본 규정의 일반 조건을 명시할 수 있고, 컨트롤러, 처리 대상인 개인정보의 유형, 관련 정보주체, 해당 개인정보를 제공받을 수 있는 기관, 목적제한, 보관기간 및 적법하고 공정한 처리를 보장하기 위한 기타 조치를 결정하는 세부사항을 수립할 수 있다. 또한 유럽연합 또는 회원국 법률은 공익을 위하거나 공적 권한 행사에 따른 직무를 수행하는 컨트롤러가 공법에 적용받는 공공기관이나 기타 자연인 또는 법인이어야 하는지 여부, 또는 공중보건, 사회적 보호, 의료서비스 관리 등 건강목적을 포함해 공익에 부합하는 경우에는 전문가협회 등 민법에 적용받는지 여부를 결정하여야 한다.

(46) 개인정보의 처리는 정보주체의 생명 또는 타인의 생명과 관련한 주요 이익을 보호하기 위하여 필요한 경우 합법적으로 간주된다. 타인의 생명과 관련한 주요 이익에 근거한 개인정보 처리는 원칙적으로 해당 처리가 명백하게 다른 법적 근거에 기반 할 수 없는 경우에 한해서 행해져야 한다. 일부 유형의 처리는 공익상 중요한 근거와 정보주체의 생명에 관련된 이익에 동시에 충족시킬 수 있는데, 에를 들어 전염병과 그 확산을 모니터링하거나 자연재해 또는 인재 등 인도주의적 비상상황에서 인도주의적 목적으로 처리가 필요한 경우가 이에 해당한다.

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

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

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

(50) 원래 수집 목적 이외의 개인정보 처리는 해당 개인정보의 처리가 원래의 수집 목적과 양립되는 경우에 한해서만 허용되어야 한다. 목적이 양립하는 경우, 당초 개인정보 수집을 허용한 법적 근거 이외의 별도의 법적 근거는 불필요하다. 공익을 추구하거나 컨트롤러에게 내재된 공적 권한의 행사에 따른 직무 수행에 처리가 필요한 경우, 유럽연합 또는 회원국 법률은 추가 처리가 양립 가능하고 적법하다고 간주되는 직무 및 목적을 결정하여 명시할 수 있다. 공익상의 기록보존 목적, 과학적 또는 역사적 연구 목적, 또는 통계 목적의 추가 처리는 양립 가능하고 적법한 처리 작업으로 간주되어야 한다. 유럽연합 또는 회원국 법률이 규정하는 개인정보 처리의 법적 근거는 추가 처리의 법적 근거도 될 수가 있다. 추가 처리의 목적이 당초 개인정보의 수집 목적과 양립되는지 여부를 확인하기 위해 컨트롤러는 당초 처리의 적법성에 관한 모든 요건을 충족시킨 후 무엇보다 당초 수집목적과 추가 처리 목적 간의 연관성, 해당 개인정보가 수집될 때의 상황, 특히 정보주체가 컨트롤러와의 관계를 토대로 추가 사용에 대해 합리적으로 예상할 수 있는 바, 해당 개인정보의 성격, 예정된 추가 처리가 정보주체에게 미치는 결과, 당초 처리 작업 및 추가 처리 작업에 대한 적절한 안전장치의 유무를 고려하여야 한다.

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

(51) 본질적으로 기본권과 자유와 관련해 특히 민감한 개인정보는 그 처리가 기본권 및 자유에 중대한 위험을 초래할 수 있기 때문에 특정한 보호를 받아야 한다. 이러한 정보에는 인종 또는 민족출신을 드러나는 개인정보도 포함되어야 하나, 본 규정에서 '인종출신'이라는 용어를 사용한다고 하여 유럽연합이 서로 다른 인종이 존재한다고 단정 지으려는 이론을 용인한다는 의미는 아니다. 사진의 처리는 개인을 고유하게 식별하거나 인증할 수 있는 특정 기술 수단을 통해 처리될 시에만 생체정보의 정의에 해당되기 때문에, 체계적으로는 특별 범주의 개인정보 처리로 분류되지 않는다. 그 개인정보는 회원국의 법률이 공익을 위하거나 컨트롤러에 부여된 공적 권한 행사에 따른 직무 수행 또는 법적 의무의 준수를 위해 본 규정의 규칙 적용을 변경하고자 데이터 보호에 관한 특정 조문을 규정할 수 있다는 사실을 고려하여 본 규정에 명시된 특정 상황에서 허용되지 않는다면 처리되어서는 안 된다. 그 처리에 대한 특정 요건과 더불어, 본 규정의 통칙 및 기타 규칙은 특히 적법한 처리를 위한 조건과 관련하여 적용되어야 한다. 그 같은 특별 범주의 개인정보 처리를 일반적으로 금지하는 것에 대한 적용제외는 명시적으로 제공되어야 하고, 특히 정보주체가 명백한 동의를 제공한 경우나 특히 기본적 자유 행사를 허용할 목적으로 특정 재단 또는 협회가 행하는 정당한 활동 중에 처리가 이루어지는 경우의 특정 요구조건과 관련하여 더욱 그러하다.

(52) 특별 범주의 개인정보 처리를 금지하는 것에 대한 적용제외는 유럽연합 또는 회원국 법률에 규정이 되어있고 적절한 안전장치에 따를 경우 개인정보 및 기타 기본권 보호를 위해 허용되어 한다. 특히 공익을 위한 경우로서, 고용법, 연금 및 의료보장 등의 사회적 보호 법률, 감시 및 경계 목적, 전염병 및 기타 건강에 대한 중대한 위협을 예방하거나 통제하려는 경우의 개인정보 처리에 대해서 특히 적용제외가 허용이 되어야 한다. 그 같은 적용제외는 공중보건, 의료 서비스 관리 등의 보건 목적을 위해 허용될 수 있으며, 특히 건강보험 제도상 수당 및 서비스 청구에 사용되는 절차의 품질 및 비용의 효율성을 보장하기 위해서나 공익적 기록보존 목적, 과학적 및 역사적 연구 목적 또는 통계 목적을 위해 허용될 수 있다. 적용제외는 또한 법적 청구권(legal claims)의 입증, 행사 또는 방어 시 필요한 경우 '법정 소송절차, 행정절차 또는 법원 외 절차인지 여부에 관계없이' 그러한 특별 범주의 개인정보 처리를 허용하여야 한다.

(53) 더 높은 수준의 보호를 받아야 하는 특별 범주의 개인정보는 개인 및 사회 전반의 이익을 위한 목적 달성에 필요한 건강 관련 목적으로만 처리되어야 하며, 특히 품질관리, 관리정보, 의료서비스 및 사회보장 제도에 대한 국가와 지역차원의 감독 목적, 의료서비스나 사회보장의 지속성 및 국가간 의료서비스나 의료보장 달성의 목적, 모니터링 및 경계 목적이나 공익적 목표를 달성해야 하는 유럽연합 또는 회원국 법률에 근거한 공익적 기록보존 목적, 과학적 또는 역사적 연구 목적이나 통계 목적을 위해, 그리고 공중보건 부문의 공익을 위한 연구를 위해 경영진 및 중앙 보건당국이 그 같은 데이터를 처리하는 등 의료서비스 또는 사회보장서비스·제도를 관리하는 경우에서 개인과 사회 전체의 이익을 위해 그 목적 달성이 필요한 경우가 그러하다. 따라서 본 규정은 특히 직무상의 법적 기밀유지 의무가 보장되는 상황에서 개인이 특정의 건강 관련 목적으로 건강에 관한 특별 범주의 개인정보를 처리하는 경우, 특정 니즈(needs)를 고려하여, 그 같은 처리에 대한 조화로운 여건을 제공하여야 한다. 유럽연합 또는 회원국 법률은 개인의 기본권 및 개인정보를 보호하기 위한 구체적이고 적절한 조치를 규정하여야 한다. 회원국은 유전 정보, 생체 정보 또는 건강에 관한 데이터의 처리와 관련하여 제한 등 추가적 조건을 유지하거나 도입할 수 있어야 한다. 그러나

회원국 간에 이루어지는 그 같은 처리에 상기 조건이 적용될 시 유럽연합 역내의 자유로운 개인정보 이동이 방해를 받아서는 안 된다.

(54) 특별 범주의 개인정보 처리는 정보주체의 동의 없이 공중보건 분야에서 공익상의 이유로 필요할 수 있다. 그 처리는 개인의 권리와 자유를 보호하기 위해 적절하고 구체적인 조치를 적용받아야 한다. 그러한 맥락에서 '공중보건'은 유럽의회와 각료이사회의 규정(EC) No1338/2008에 정의된 대로 해석되어야 하며, 이는 건강과 관련된 모든 요소로서 질병 상태나 장애 등의 건강상태, 그 건강상태에 영향을 미치는 결정적 요소, 의료서비스의 필요, 의료서비스에 할당된 자원, 의료서비스 지출 및 재정 조달을 비롯한 의료서비스 제공 및 보편적 이용, 그리고 사망 원인 등을 가리킨다. 공익적 사유의 그 같은 건강 관련 개인정보의 처리로 인해 고용인 또는 보험사, 그리고 금융사 등 제3자가 기타 목적으로 개인정보를 처리하는 결과가 초래되어서는 안 된다.

(55) 또한 헌법이나 국제공법에 규정된 공인된 종교단체의 목표를 달성할 목적으로 공공당국이 실시하는 개인정보의 처리는 공익을 근거로 시행된다.

(56) 선거활동 중 회원국 내 민주주의 제도의 작동을 위해 정당이 개인의 정견에 대한 개인정보를 축적하도록 요구되는 경우, 적절한 안전조치가 수립되는 한, 공익의 사유로 그 같은 데이터의 처리가 허용될 수 있다.

(57) 컨트롤러는 본인이 처리하는 개인정보를 통해 개인을 식별할 수 없는 경우, 본 규정 조문 일체의 준수라는 유일한 목적만으로 정보주체를 식별하기 위한 추가 정보를 취득해야 할 의무가 없다. 그러나 컨트롤러는 정보주체가 본인의 권리의 행사를 지원하고자 제공하는 추가 정보의 수령을 거부해서는 안 된다. 식별에는 정보주체가 컨트롤러가 제공하는 온라인 서비스에 로그인 시 사용하는 것과 동일한 증명서 등의 인증 메커니즘을 통한 디지털 신원확인도 포함된다.

(58) 투명성의 원칙에 따라 대중 또는 정보주체에 제공되는 정보는 간결하고 이용이 용이하며 이해하기 쉬워야 하고, 명확하고 평이한 언어의 사용에 더해 적절한 경우 시각화 기법을 활용해야 한다. 그 같은 정보는 대중에게 제공될 시 웹사이트를 통해 전자 양식으로 제공될 수 있다. 이는 온라인 광고 등 활동주체(actors)의 확산 및 관행의 기술적 복잡성으로 인해 정보주체가 누가 무슨 목적으로 본인에 관한 개인정보를 수집하는지 여부를 파악하기 어려운 상황과 특히 관련이 있다. 아동에게 특정한 보호수단이 필요하다는 것을 고려할 때 아동을 대상으로 한 (데이터)처리 시 정보제공 및 통지 일체는 해당 아동이 쉽게 이해할 수 있는 명확하고 평이한 언어로 이루어져야 한다.

(59) 개인정보의 열람, 정정 또는 삭제를 요청하고 적용 가능한 경우 이를 무상으로 획득할 메커니즘 등 본 규정에 따른 정보주체의 권리 행사 및 반대할 권리 행사를 지원할 양식(modalities)이 제공되어야 한다. 컨트롤러는 특히 전자 수단에 의해 개인정보가 처리되는 경우, 전자적 방식으로 요청을 할 수 있는 방법도 제공하여야 한다. 컨트롤러는 부당한 지체 없이, 늦어도 한 달 이내에 정보주체의 요청에 응대하여야 하며 정보주체의 요청에 응하지 않으려는 경우, 그 사유를 제공할 의무가 있다.

(60) 공정하고 투명한 처리의 원칙에 따라 정보주체는 처리 작업의 존재 및 그 존재에 대하여 통지 받아야 한다. 컨트롤러는 개인정보가 처리되는 특정 상황 및 맥락을 참작하여 공정하고 투명한 처리 보장에 필요한 모든 추가적인 정보를 정보주체에 제공해야 한다. 또한 정보주체는 프로파일링 유무와 해당 프로파일링의 결과에 대해 통지받아야 한다. 정보주체로부터 개인정보가 수집되는 경우, 해당 정보주체는 본인이 개인정보 제공의 의무가 있는지 여부 및 해당 정보를 제공하지 않을 경우의 결과에 대해 통지받아야 한다. 그 정보는 눈에 잘 띄고 이해하기 쉬우며 가독성이 뛰어난 방식으로 예정된 처리에 대해 중요한 개략적 정보를 제공하기 위해 표준화된 아이콘과 함께 제공될 수 있다. 전자 수단을 이용하여 아이콘을 제공하는 경우에는 기계 판독이 가능해야 한다.

(61) 정보주체에 관한 개인정보의 처리와 관련한 정보는 정보주체로부터 수집 당시 또는 제3의 출처로부터 정보가 수집된 경우 적절한 기간 내에, 해당 경우의 상황에 따라, 정보주체에 제공되어야 한다. 개인정보가 합법적으로 제3의 수령인에게 제공될 수 있는 경우, 해당 정보주체는 정보가 최초로 해당 수령인에게 제공될 시 이를 통지받아야 한다. 컨트롤러가 당초 수집 목적 외로 개인정보를 처리하려는 경우, 컨트롤러는 추가 처리에 앞서 정보주체에게 추가 목적에 대한 정보 및 기타 필요한 정보를 제공해야 한다. 다양한 출처의 활용으로 인해 정보주체에게 개인정보의 출처를 제공할 수 없는 경우, 일반적인 정보가 제공되어야 한다.

(62) 그러나 정보주체가 이미 해당 정보를 보유하고 있는 경우, 법률이 해당 개인정보의 기록 또는 제공을 명백히 규정한 경우, 또는 정보주체에 해당 정보를 제공하는 것이 불가능하다고 입증되거나 비례하지 않는 노력을 요하는 경우에는 정보 제공의 의무를 부과할 필요가 없다. 후자는 특히 공익적 기록보존 목적, 과학적 또는 역사적 연구 목적, 또는 통계 목적으로 처리가 실시되는 경우가 해당될 수 있다. 이와 관련해 정보주체의 수, 해당 개인정보의 생성시점 및 채택된 모든 적절한 안전장치가 고려되어야 한다.

(63) 정보주체는 처리의 적법성을 인지하고 검증하기 위해 본인에 관해 수집된 개인정보를 열람하고 그 권리를 용이하게, 그리고 적절한 시간 간격으로 행사할 권리를 가진다. 권리를 가진다. 정보주체가 진단, 검사 결과, 의료진의 평가, 제공된 치료나 조치 등의 정보가 포함된 의료 기록상의 데이터 등 본인의 권강에 관한 데이터를 열람할 권리도 이에 포함된다. 따라서 모든 정보주체는 특히 개인정보가 처리되는 목적, 가능한 경우 처리기간, 개인정보의 수령인, 개인정보 자동 처리에 수반되는 논리, 처리가 프로파일링을 근거로 할 시 최소한 그 처리 결과에 대해 알고 전달(통지)받을 권리를 가진다. 가능한 경우, 컨트롤러는 보안시스템에 대한 원격 접속을 가능하게 하여 정보주체가 본인의 개인정보를 직접 열람하게 할 수 있다. 그 권리가 거래 기밀이나 지적재산권, 그리고 특히 소프트웨어 보호 저작권 등 타인의 권리와 자유에 악영향을 끼쳐서는 안 된다. 그러나 상기 사항을 고려함으로 인해 정보주체에게 일체의 정보를 제공하는 것이 거부되어서는 안 된다. 컨트롤러가 정보주체에 관한 대량의 정보를 처리하는 경우, 컨트롤러는 그 정보를 전달하기 전에 정보주체가 해당 요청에 관련된 정보 또는 처리 활동을 명시하도록 요구할 수 있다.

(64) 컨트롤러는 특히 온라인 서비스 및 온라인 식별자와 관련한 상황에서 열람을 요구한

정보주체의 신원을 확인하기 위한 모든 적정 조치를 취해야 한다. 컨트롤러는 잠재적 요청을 응대한다는 유일한 목적으로 개인정보를 보유해서는 안 된다.

(65) 정보주체는 본인에 관한 개인정보를 보관하는 것이 본 규정이나 컨트롤러에 적용되는 유럽연합 또는 회원국 법률을 침해하는 경우, 그 정보를 정정할 권리 및 '잊힐 권리'를 가진다. 특히 정보주체는 본인의 개인정보가 수집되거나 달리 처리되는 목적과 관련하여 더 이상 필요하지 않은 경우, 정보주체가 본인에 관한 개인정보의 처리에 대한 동의를 철회하였거나 반대하는 경우, 본인의 개인정보에 대한 처리가 기존과는 달리 본 규정을 준수하지 않는 경우 그 정보를 삭제할 권리와 그 정보가 더 이상 처리되지 않도록 할 권리를 가진다. 그 권리는 특히 정보주체가 아동으로서 본인의 동의를 제공하였고. 처리에 관여된 위험을 완전히 인지하지 못하다가 이후 특히 인터넷상에서 그 개인정보를 삭제하기를 희망하는 경우와 관련 있다. 그 정보주체가 더 이상 아동이 아닐지라도 이 권리를 행사할 수 있어야 한다. 그러나 개인정보의 추가 보관은 필요한 경우 적법하며, 표현 및 정보의 자유권 행사, 법적 의무 준수, 공익을 위하거나 컨트롤러에 부여된 공적 권한 행사에 따른 직무 수행, 공중보건 분야의 공익적 근거, 공익적 기록보존 목적, 과학적 또는 역사적 연구 목적이나 통계 목적, 또는 법적 청구권의 입증, 행사, 방어를 위한 경우가 이에 해당한다.

(66) 온라인 환경에서의 잊힐 권리 강화를 위해서는 개인정보를 공개한 컨트롤러가 그 개인정보를 처리 중인 컨트롤러에게 해당 개인정보에 대한 링크, 사본, 복제물을 삭제하도록 통지할 의무를 지니는 방식으로 삭제권을 확대하여야 한다. 그렇게 함에 있어 컨트롤러는 해당 개인정보를 처리 중인 컨트롤러에게 정보주체의 요청을 통지하기 위한 기술 조치 등 컨트롤러가 가용할 수 있는 기술 및 방법을 고려하여 적절한 조치를 취해야 한다.

(67) 개인정보 처리를 제한하는 방법에는 특히 선택된 정보를 기타 처리 시스템으로 임시 이전시키거나 선택된 정보를 이용자가 열람하지 못하게 하거나 공개된 개인정보를 웹사이트에서 임시 삭제하는 것이 포함될 수 있다. 자동화 파일링시스템에서 처리 제한은 원칙적으로 개인정보가 추가 처리되지 않고 변경되지 않는 방식으로 기술적 수단에 의해 보장되어야 한다. 개인정보 처리가 제한된다는 사실은 시스템 내에 명백하게 표시되어야 한다.

(68) 본인의 데이터에 대한 통제를 더욱 강화하기 위해 개인정보가 자동수단을 통해 개인정보가 처리되는 경우 정보주체는 컨트롤러에게 제공한 본인의 개인정보를 조직적이고 상용화된, 기계판독 및 상호운용이 가능한 형식으로 수령하고 이를 제3의 컨트롤러에게 이전할 수 있어야 한다. 컨트롤러는 데이터 이동권data portability)을 가능하게 하는 상호운용 가능한 포맷을 개발하도록 장려된다. 그 권리는 정보주체가 본인의 동의에 근거하여 개인정보를 제공한 경우나 계약의 이행에 처리가 필요한 경우에 적용되어야 한다. 처리가 동의 또는 계약 이외의 법적 근거를 기반으로 하는 경우에는 그 권리가 적용되지 않는다. 그 권리는 본질적으로 공적 업무 수행을 위해 개인정보를 처리하는 컨트롤러에 반(反)하여 행사되어서는 안 된다. 따라서 컨트롤러에게 적용되는 법적 의무를 준수하기 위해 또는 공익을 위하거나 컨트롤러에게 부여된 공적 권한의 행사에 따른 직무 수행에 개인정보가 필요한 경우에는 그 권리가 적용되어서는 안 된다. 본인의 개인정보를 이전하거나 수령할 정보주체의 권리로 인해 컨트롤러에게 기술적으로 양립되는 처리 시스템을 채택하거나 유지해야 할 의무가 부과되어서는 안 된다. 특정 개인정보 세트에서 복수의 정보주체가 관련되는 경우, 개인정보를

수령할 권리는 본 규정에 따른 타 정보주체의 권리와 자유를 침해해서는 안 된다. 또한 그 권리는 정보주체 본인의 개인정보 삭제권과 그 권리에 대해 본 규정이 정한 제한을 침해해서는 안 되며, 특히 계약 이행에 개인정보가 필요한 범위 및 기간에 한하여 정보주체 본인이 제공한 개인정보에 대한 삭제를 의미하는 것이 아니다. 기술적으로 가능한 경우 정보주체는 해당 개인정보를 한 컨트롤러로부터 또 다른 컨트롤러에게 직접 이전할 수 있는 권리를 가진다.

(69) 공익을 위하거나 컨트롤러에 부여된 공적 권한 행사에 따른 직무 수행에 처리가 필요하거나 컨트롤러 또는 제3자의 정당한 이익에 근거하여 처리가 필요한 이유로써 개인정보의 처리가 적법할 수 있는 경우, 정보주체는 그럼에도 불구하고 본인의 특정 상황과 관련한 어떤 개인정보의 처리에라도 반대할 권한이 있다. 컨트롤러가 가지는 설득력 있는 정당한 이익이 정보주체의 이익이나 기본권 및 자유에 우선한다는 것을 입증하는 것은 컨트롤러의 책임이다.

(70) 직접 마케팅을 목적으로 개인정보를 처리하는 경우, 정보주체는 최초 또는 추가 처리와 관련 있는지 여부에 상관없이 그 처리가 해당 직접 마케팅에 관계되는 선에서 언제라도 무상으로 프로파일링을 포함, 그 같은 처리에 반대할 권리를 가진다. 그 권리에 대해 정보주체에게 명시적으로 알려야 하며 기타 정보와는 별도로 명백하게 제시되어야 한다.

(71) 정보주체는 온라인 신용신청의 자동 거절이나 인적개입 없이 이루어지는 전자채용 관행 등 자동화 처리에만 근거하여 본인에 관한 개인적인 면을 평가하고 본인에게 법적인 영향 또는 유사하게 중대한 영향을 초래하는 조치를 포함할 수 있는 결정에 따르지 않을 권리를 가진다. 그 처리에는 개인에 관한 개인적인 측면을 평가하는 모든 형태의 개인정보 자동화 처리로 구성된 '프로파일링'이 포함되고, 특히 정보주체의 업무능력, 경제적 상황, 건강, 개인의 선호나 관심사, 신뢰성 또는 행동, 위치나 움직임에 관한 측면을 분석 또는 예측하며, 정보주체에게 법적인 영향이나 이에 상응하는 중대한 영향을 미치는 경우 그러하다. 그러나 프로파일링 등 그러한 처리에 근거한 의사결정은 컨트롤러가 적용받는 유럽연합 또는 회원국 법률에서 명시적으로 승인하는 경우 허용되어야 하며, 유럽연합 산하기구 또는 회원국 감독기구의 규정, 기준 및 권고에 따라 실시되는 사기 및 탈세의 감시·예방 목적으로나 컨트롤러가 제공하는 서비스의 보안 및 신뢰성을 보장하기 위해, 또는 정보주체와 컨트롤러 간의 계약 체결이나 이행에 필요하거나 정보주체가 명시적인 동의를 제공하였을 때 등이 이에 해당한다. 어떠한 경우에도, 그러한 처리는 정보주체에게 제공되는 특정 정보, 인적개입을 획득할 권리, 견해를 표현할 권리, 상기 평가 후 내려진 결정에 대한 설명을 얻을 권리, 해당 결정에 이의를 제기할 권리 등 적절한 안전장치를 적용받아야 한다. 그 같은 조치에 아동은 관여되지 않는다.

정보주체와 관련하여 공정하고 투명한 처리를 보장하기 위해서, 컨트롤러는 개인정보가 처리되는 특정 상황과 맥락을 고려하여 프로파일링을 위한 적절한 수학적 또는 통계적 절차를 사용하고, 특히 개인정보를 부정확하게 만드는 요인을 시정하고 오류의 위험을 최소화시키는 데 적절한 기술적 및 관리적 조치를 이행하며, 정보주체의 이익과 권리를 위해 관련된 잠재적 위험을 고려하고 특히 인종이나 민족출신, 정견, 종교나 신념, 노동조합의 가입여부, 유전적 상태나 건강 상태, 또는 성적취향에 근거하여 개인에 미치는 차별을 방지하는 방식

또는 그 같은 효과를 지니는 조치가 이루어지는 방식으로 개인정보를 보호해야 한다. 특별 범주의 개인정보에 근거한 자동 의사결정 및 프로파일링은 특정 조건에 따라서만 허용되어야 한다.

(72) 프로파일링은 처리의 법적 근거 또는 데이터 보호원칙 등 개인정보 처리와 관련한 본 규정의 규칙을 적용받는다. 본 규정에 따라 설립된 유럽 데이터보호이사회('이사회')는 그 같은 맥락에서 지침을 발간할 수 있어야 한다.

(73) 특정 원칙 및 정보를 제공받을 권리(right of information)에 대한 제재, 개인정보에 대한 접근권·정정권·삭제권에 대한 제재 및 정보 이동권에 대한 제재, 반대권, 프라이파일링에 근거한 결정에 대한 제재와 정보주체로의 개인정보 침해사고 통지(communication) 권리 및 컨트롤러의 특정 관련 의무에 대한 제재가 유럽연합법 또는 회원국 법률에 의해 부과될 수 있다. 특히 자연재해나 인재로부터 인간의 생명을 보호하고, 범죄 예방·조사·기소나 형서 처분의 수행 등 공안을 보호하고, 공안에 대한 위협으로부터 보호하거나 예방하며, 직업의 윤리 규정에 대한 위반을 예방하고, 유럽연합이나 회원국의 일반적인 공익이라는 다른 중요한 목표 및 경제적 또는 재정적 특정 원칙의 위반을 예방하고, 일반 공익상의 이유로 보관한 공개 기록부(public registers)를 관리하고, 이전 전체주의 국가에서 자행되었던 정치적 행위에 대한 구체적인 정보를 제공하기 위해 보관된(archived) 개인정보를 추가 처리하거나, 사회 보호·공중보건·인도주의적 목적 등, 정보주체를 보호하거나 타인의 권리와 자유를 보호하기 위해 민주사회에서 필요하고 비례하다고(proportionate) 생각되는 경우일 때 이러한 제재가 가능하다. 상기의 제재는 헌장 및 인간의 권리 및 기본적 자유보호에 대한 유럽 협약(European Convention for the Protection of Human Rights and Fundamental Freedoms)에 규정된 요건을 반드시 준수해야 한다.

(74) 컨트롤러가 수행하는 개인정보 처리나 컨트롤러를 대신하여 수행하는 개인정보의 처리에 대한 컨트롤러의 책임(responsibility and liability)이 수립되어야 한다. 특히 컨트롤러는 적절하고 효과적인 조치를 시행할 의무를 지녀야하며 조치의 효력 등, 본 규정에 따라 처리활동을 하고 있음을 입증할 수 있어야 한다. 이러한 조치는 개인정보처리의 성격, 범위, 상황, 목적 그리고 개인의 권리와 자유에 초래되는 위험요소를 고려해야 한다.

(75) 개인의 권리와 자유에 초래되는 위험은, 다양한 발생가능성과 심각성으로 나타나는데 이는, 개인정보 처리로 인해 발생할 수 있으며, 이는 신체적(physical), 물질적(material) 혹은 비-물질적(non-material) 손해를 초래할 수 있다. 특히, 처리로 인해 차별, 신용도용 및 사기, 재정적 손실, 명예훼손, 직무상의 기밀로 보호되던 개인정보의 기밀성 상실, 가명정보에 대한 무단 재식별 처리, 또는 기타의 심각한 경제적 또는 사회적 불이익이 초래될 수 있는 경우 그러하다. 또한, 정보주체가 본인의 권리와 자유를 빼앗길 수 있는 경우나, 본인의 개인정보에 대한 자기결정권(right to control) 행사하지 못하게 되는 경우, 혹은 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 관련한 보안 조치를 드러내는 방식으로 처리되는 경우. 또는 개인적인 측면에 평가되는 경우로 특히 업무능력, 경제적 상황, 건강상태, 개인의 성향 및 관심사, 신뢰성이나 행동, 위치 및 이동경로와 관련된 측면을 개인프로필 생성 및 이용을 위해 분석하거나 예측하는 경우. 혹은 아동

등 취약한 개인의 개인정보가 처리되는 경우나 처리가 방대한 양의 개인정보와 관련 있거나, 수많은 정보주체에게 영향을 미치는 경우가 그러하다.

(76) 정보주체의 권리와 자유에 초래될 수 있는 위험 가능성과 심각성은 해당 처리의 성격, 범위, 상황 및 목적을 참고하여 결정되어야 한다. 위험성은 개인정보 처리 작업(operation)이 위험요소 또는 높은 수준의 위험요소에 관련되었는지를 입증 하기위한 객관적인 평가에 근거하여 평가되어야 한다.

(77) 컨트롤러나 프로세서의 적절한 조치시행 및 법률 준수여부 입증에 대한 지침, 특히 처리와 관련된 위험에 대한 식별, 위험요소의 출처·성격·가능성·심각성을 고려한 평가, 그리고 위험을 완화하는 모범 방침의 모색에 대한 지침은 인가된 행동강령(approved code of conducts) 및 인증서(certificates), 또는 EDPB에서 제공하는 가이드라인이나 DPO가 제공하는 지표를 통해 제공될 수 있다. EDPB는 개인의 권리와 자유에 고위험을 초래하지 않을 것으로 간주되는 처리 작업에 대한 가이드라인을 발간할 수 있으며, 어떠한 조치로 이러한 위험요소를 충분히 해결할 수 있는 지 설명할 수 있다.

(78) 개인정보 처리에 관련된 개인의 권리와 자유를 보호하기 위해서는, 이 규정의 요건을 충족하기 위해 적절한 기술적·관리적 조치가 시행될 것이 요구된다. 이 법을 준수하고 있음을 입증하기 위해, 컨트롤러는 데이터보호설계 및 기본설정의 원칙을 만족하는 내부 정책과 조치를 채택하고 시행해야 한다. 이러한 조치에는 개인정보처리의 최소화, 가능한 빠른 시일 내의 개인정보 가명처리, 개인정보의 기능 및 처리의 투명성 제고, 개인정보 처리에 대한 정보주체의 감시 허용과 컨트롤러의 보안 대책의 수립 및 개선이 포함될 수 있다. 개인정보 처리에 근거하거나 관련 업무를 위해 개인정보를 처리하는 어플리케이션·서비스·제품을 개발, 디자인·선택·이용할 때, 해당 제품·서비스·어플리케이션의 제작자는 관련 제품·서비스·어플리케이션을 개발하고 디자인할 때, 개인정보보호권을 고려하고, 컨트롤러와 프로세서는 개인정보보호 의무를 준수할 수 있도록 보장하도록 권장된다. 데이터 보호 설계 및 기본설정의 원칙은 대중이 선호하는 관점(in the context of public tenders)에서 생각했을 때에도 고려되어야 한다.

(79) 감독기관의 모니터링 및 조치와 관련하여서도, 정보주체의 권리와 자유에 대한 보호 및 컨트롤러와 프로세서의 책임에 대한, 본 규정에 따른 명확한 책임 분배가 필요하다. 여기에는 컨트롤러가 다른 컨트롤러와 공동으로 처리의 목적과 수단을 결정할 수 있는 경우나 컨트롤러를 대신하여 처리작업을 수행할 수 있는 경우가 포함된다.

(80) 유럽연합 역외에 설립된 컨트롤러 또는 프로세서는 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 컨트롤러 또는 프로세서는 대리인을 지정해야 하지만, 처리가 간헐적이고(occasional), 대규모의 처리나 특별범주의 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 컨트롤러가 공공기관이나 기구인 경우는 예외로 한다. 대리인은 컨트롤러와

프로세서를 대신하여 행동해야 하며 감독기관이 지정할 수 있다. 대리인은 컨트롤러 또는 프로세서의 공식 위임서한을 통해 명확하게 지정되어 이 규정에 규정된 의무를 대신 이행한다. 이러한 대리인의 지정은 이 규정에 규정된 컨트롤러 또는 프로세서의 책임(responsibility and liability)에는 영향을 미치지 않는다. 해당 대리인은 컨트롤러에게 부여받은 권한에 따라 대리인으로써 업무를 수행해야하며, 여기에는 이 법을 준수하기 위해 적용된 모든 조치와 관련하여 관할 감독기관과 협력하는 것이 포함된다. 지정된 대리인은 컨트롤러 또는 프로세서가 규정을 준수하지 않은 경우, 집행절차를 적용받아야 한다.

(81) 컨트롤러를 대신하여 프로세서 수행하는 처리와 관련하여, 이 규정을 준수하도록 보장하기 위해서, 프로세서에게 처리 활동을 위탁할 때, 컨트롤러는 전문적 지식, 신뢰성 및 자원과 특히 관련하여, 처리 보안 등, 이 규정의 요건을 맞출 수 있는 기술적 및 관리적 조치를 시행한다는 충분한 확신을 제공하는 프로세서만을 활용해야 한다. 프로세서의 승인된 행동강령이나 공인 인증 메커니즘에 대한 준수는 컨트롤러의 의무의 준수를 입증하는 요소로 이용될 수 있다. 프로세서의 개인정보 처리의 수행은 유럽연합 또는 회원국 법률에 규정된 계약 또는 기타 법률에 적용받아야 하며, 이를 통해 프로세서는 컨트롤러에게 구속되고, 처리 사안(subject-matter) 및 처리기간, 처리의 성격 및 목적, 개인정보 유형 및 정보주체의 범주를 규정하고 있어야하며, 수행되는 개인정보 처리 상황에서의 프로세서의 구체적인 업무 및 책임과 정보주체의 권리와 자유에 대한 위험요소를 고려해야 한다. 컨트롤러와 프로세서는 개별 계약 방식 또는 위원회가 채택하거나, 감독기관이 일관성 메커니즘에 따라 채택 후 위원회가 채택한 표준 계약 조항(standard contractual clauses) 방식 중 하나의 방식을 선택할 수 있다. 컨트롤러를 대신하여 처리를 완료한 후, 프로세서는, 컨트롤러의 선택에 따라, 관련 개인정보를 반환 또는 파기해야하지만, 프로세서가 적용받는 유럽연합 또는 회원국 법률에 따라 개인정보를 보관하라는 요구사항이 있는 경우는 예외로 한다.

(82) 이 규정의 준수를 입증하기 위해, 컨트롤러 또는 프로세서는 책임을 갖고 처리 활동 기록을 관리해야 한다. 컨트롤러와 프로세서 각각은 감독기관과 협력할 의무를 지녀야 하며, 이러한 처리작업에 대한 모니터링을 하기 위해, 요청 시 해당 자료를 열람가능하게 해야한다.

(83) 보안을 유지하고 이 규정을 위반하는 처리를 예방하기 위해, 컨트롤러 또는 프로세서는 처리에 내재된 위험요소를 평가하고, 해당 위험요소를 완화할 수 있는 암호처리 등의 조치를 시행해야 한다. 이러한 조치는 보호되어야 할 개인정보의 성격과 위험에 비례하여 (조치) 시행의 수준(state of the art)과 비용을 고려한 후 기밀성 보장 등, 적절한 보안 수준을 보장해야 한다. 개인정보의 보안위험요소를 평가할 때, 개인정보 처리로 초래되는 위험에 대해 고려해보아야 하며, 예를 들면 특히 신체적, 물질적 그리고 비-물질적 피해를 초래할 수 있는 위험으로, 이전되거나 저장된 개인정보 혹은 다르게 처리된 개인정보의 사고적 혹은 불법적 파기, 손실, 변경, 무단 제공 혹은 무단 열람 등이 있다.

(84) 처리 방법이 개인의 권리와 자유에 관해 높은 수준의 위험을 초래할 가능성이 있는 경우 이 규정을 보다 더 잘 준수하기 위해서, 컨트롤러는 특히 관련 위험의 출처, 성격, 특성 그리고 심각성을 평가하는 개인정보보호 영향평가(DPIA)를 수행할 책임이 있다. 평가결과는, 이 규정에 따라 개인정보가 처리되었음을 입증하기 위해 적절한 조치를 결정할 때, 고려되

어야 한다. 개인정보보호 영향평가 결과를 통해, 컨트롤러가 이용할 수 있는 기술과 기술시행 비용을 고려했을 때, 적절한 조치로 고위험을 완화할 수 없는 처리 작업임이 판단되는 경우, 처리 이전에 감독기관에 자문을 구해야 한다.

(85) 개인정보 유출사고가 적절하고 시의 적절하게 해결되지 않을 경우, 개인은 본인의 개인정보에 대한 자기결정권 상실이나 권리 제한, 차별, 신원도용 및 신용사기, 재정적 손실, 가명처리의 무단 재식별, 명예훼손, 직무상 비밀로 지켜지던 개인정보의 기밀성 상실과 기타 경제적 또는 사회적 불이익 등과 같은 신체적, 물질적 그리고 비(非) 물질적 피해를 입을 수 있다. 따라서 컨트롤러는 개인정보 유출을 알게 되는 즉시 지체 없이 가능한 72시간 이내에 관련 감독기관에 이 사실을 신고해야 한다. 그러나 컨트롤러가, 책임성의 원칙에 따라, 해당 개인정보의 유출이 개인의 권리와 자유에 관해 위험요소를 초래할 가능성이 낮다고 입증할 수 있는 경우는 예외로 한다. 해당 유출사고의 통지가 72시간 이내에 이루어지지 않을 경우, 지체된 이유는 통지내용과 함께 제공되고 관련 정보는 부당한 지체 없이 단계별로 제공될 수 있다.

(86) 컨트롤러는 개인정보 유출이 개인의 권리와 자유에 고위험을 초래할 가능성이 있는 경우, 정보주체가 필요한 예방조치를 취할 수 있도록 부당한 지체 없이 개인정보의 유출을 정보주체에게 통지해야 한다. 통지에는 유출된 개인정보의 성격과 잠재적인 부작용을 완화할 수 있는 권고대책이 포함되어야 한다. 통지는 합리적으로 가능한 빨리, 감독기관 또는 법집행기관 등 기타 관련 기관이 제공하는 지침에 따라 해당 감독기관과의 긴밀한 협력 아래에 이루어져야 한다. 예를 들어, 즉각적으로 피해를 줄이기 위한 경우, 정보주체에 즉시 통지해야 하는 한편, 지속적이거나 비슷한 개인정보의 유출을 막기 위해 적절한 조치를 취해야 하는 경우는 통지하기까지 더 오랜 시간 소요되는 것을 정당화 할 수 있다.

(87) 개인정보 유출 발생여부를 즉각적으로 입증하기 위해 적절한 기술적 보호 및 관리조치가 시행되었는지, 이를 감독기관과 정보주체에 즉시 신고했는지 여부를 확인해야 한다. 유출된 개인정보의 성격과 사고의 심각성, 정보주체에 초래되는 영향과 부작용을 특히 고려하여, 부당한 지체없이 통지가 이루어졌는지를 입증해야 한다. 이러한 통지 후, 이 규정상의 감독기관 업무와 권한에 따라, 감독기관이 개입하게 될 수도 있다.

(88) 개인정보 유출 통지의 형식 및 절차에 대한 상세한 규칙을 세우려면, 해당 유출사고 시, 적절한 기술적 보호조치를 통해 신원사기나 다른 형태의 오용의 가능성을 효과적으로 제한하여 개인정보가 보호되고 있었는지 등의 상황을 충분히 고려해야 한다. 게다가, 이러한 규칙이나 절차는 법집행기관의 정당한 이익도 고려해야 한다. 성급한 공개(early disclosure)는 유출사고 상황에 대한 조사를 불필요하게 방해할 수도 있다.

(89) 지침 95/46/EC에서는 감독기관에 개인정보처리를 통지하라는 일반적인 의무조건을 규정하고 있었다. 이러한 의무는 행정적, 재정적 부담을 주는 반면, 항상 개인정보보호 개선에 도움이 된 것은 아니었다. 따라서 이러한 무차별적인 일반적인 통지의 의무는 철폐되어야 하며, 대신 처리 작업의 성격·범위·상황·목적에 따라 개인의 권리와 자유에 고위험을 초래할 가능성이 있는 처리작업 유형을 중점적으로 통지하는, 효과적인 절차와 메커니즘으로 대체되어야 한다. 여기에 해당되는 처리작업의 유형은 신기술을 사용하는 경우나 새로운 종류의

처리인 경우, 컨트롤러가 이전에 개인정보 영향평가를 시행한 적이 없는 경우나 혹은 최초의 처리 이후 시간이 흘러 개인정보 영향평가가 필요하게 된 경우가 포함된다.

(90) 이러한 경우, 고위험의 가능성 및 강도를 평가하기 위해 처리의 성격·범위·상황·목적 그리고 위험요소의 출처를 고려하여, 처리 이전에 개인정보보호 영향평가가 컨트롤러에 의해 수행될 수 있어야 한다. 이러한 개인정보보호영향평가는 해당 위험을 완화하고 개인정보를 보호하며, 본 규정의 준수여부를 입증하기 위한 조치, 안전장치 및 메커니즘을 특히 포함해야 한다.

(91) 이는 특히 상당한 양의 개인정보를 지역적, 국가적, 초국가적 차원에서 처리하고자 하는 대규모의 처리작업과 수많은 정보주체에게 영향을 미칠 수 있는 처리작업, 그리고 현재의 기술적 지식 수준에서 신기술을 대규모 처리에 사용하는 경우 등, 그 민감성 때문에 고위험을 초래할 수 있는 처리작업뿐 아니라 정보주체가 권리를 행사하기 어려운 상황 등, 정보주체의 권리와 자유에 고위험을 초래할 수 있는 기타 처리 방식에 적용되어야 한다. 또한, 관련 개인정보의 프로파일링에 근거하여 개인의 개인적인 측면에 대한 체계적이고 광범위한 일체의 평가를 따라 특정 개인에 대한 결정을 내리기 위해 개인정보를 처리하는 경우, 혹은 특별범주의 개인정보, 생체정보 또는 형사기소 및 범죄나 관련보안조치에 대한 정보처리에 따라 특정 개인에 대한 결정을 내리기 위해 개인정보를 처리하는 경우, 개인정보보호 영향평가가 이루어져야 한다. 특히 시각적 전자기기를 사용하여 공공장소를 대규모로 감시할 때나, 관할 감독기관이 판단하기에 해당 처리가 특히 정보주체가 권리를 행사하지 못하게 하거나 서비스 혹은 계약을 이용하지 못하게 하거나, 체계적으로 대규모로 수행되어 정보주체의 권리와 자유에 고위험을 초래할 가능성이 있다고 간주되는 처리작업에 모두 개인정보보호 영향평가는 동일하게 필요하다. 해당 개인정보 처리가 개인 내과 의사나 기타 의료전문인 또는 변호사의 환자나 고객으로부터의 개인정보가 관련된 처리인 경우, 대규모의 처리라고 간주되어서는 안 된다. 이 경우, 개인정보보호 영향평가는 의무여서는 안된다.

(92) 개인정보보호 영향평가가 단일 프로젝트보다 광범위하게 적용되어야, 합리적이고 경제적이라고 생각되는 상황이 있다. 예를 들어, 공공기관이나 공공기구가 동일한 적용 플랫폼이나 처리 플랫폼을 수립할 계획인 경우, 또는 여러 명의 컨트롤러가 산업분야나 부문 전반이나 비슷한 수준의 활동(horizontal activity)에 광범위하게 사용되는 동일한 적용환경이나 처리환경을 도입하려는 경우가 있다.

(93) 공공기관이나 공공기구의 업무수행 규정하는 회원국 법률 혹은 구체적인 처리작업이나 일련의 처리작업을 규제하는 회원국 법률을 채택할 때, 회원국은 처리활동을 하기 전에 이러한 평가의 수행이 필요하다고 생각할 수 있다.

(94) 개인정보보호 영향평가가, 위험요인을 완화할 수 있는 안전장치, 보안조치 및 메커니즘이 부재한 상황에서, 해당 처리가 개인의 권리와 자유에 고위험을 초래한다고 판단하고, 컨트롤러가 해당 위험은 가용할만한 기술과 이행의 비용 면에서 합리적인 수단으로 완화될 수 없다는 의견인 경우, 처리활동 시작 이전에 감독기관에 자문을 요청해야 한다. 이러한 고위험은 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 않더라도, 처리작업에 대한 금지 권한 등, 이 법에 규정된 감독기구의 업무와 권한에 따른 감독기관의 어떠한 개입도 가능해야 한다. 이러한 자문과정의 일환으로, 문제가 되는 처리와 관련해 수행되는 개인정보보호 영향평가의 결과는, 특히 개인의 권리와 자유에 관한 위험을 완화하기 위해 예상되는 조치는, 감독기관에 제출될 수 있다.

(95) 프로세서는, 필요 시 또는 요청에 따라, 개인정보보호 영향평가의 수행에서 파생되거나 감독기관과의 사전자문 활동에서 파생되는 의무를 준수하기 위해 컨트롤러를 도와야 한다.

(96) 감독기관과의 자문은 개인정보의 처리를 위해 제공되는 법적, 규제적 조치의 준비 과정에서도 이루어져야 하며, 이는 이 법에 맞는 의도된 처리를 준수하고 특히 정보주체에 관련된 위험을 완화하기 위함이다.

(97) 법원이나 독립적 사법기관이 사법적 권한에 따라 (정보)처리를 하는 경우를 제외한, 공공기관이 처리를 수행하는 경우, 민간부문에서 정보주체에 대해 주기적이고 체계적인 모니터링을 대규모로 필요로 하는 처리작업이 핵심활동인 컨트롤러가 (정보)처리를 하는 경우, 혹은 컨트롤러나 프로세서의 핵심활동이 특별 범주의 개인정보나 형사기소 및 범죄에 관련된 개인정보를 대규모로 처리 하는 경우, 개인정보보호법 및 개인정보보호 방침에 대해 전문적인 지식을 가진 자는 동 규정이 내부적으로 지켜지고 있는지 모니터링하기 위해 컨트롤러나 프로세서를 도와야 한다. 민간 부문에서의 컨트롤러 핵심 활동(core activities)은 주요 활동(primary activities)과 관련되며 보조적인 활동으로써의 개인정보처리와는 관련이 없다. 이 때 필요한 전문적 지식의 수준은, 컨트롤러나 프로세서가 수행하는 정보처리 작업과 이들이 처리한 개인정보에 필요한 보호에 따라 특히 결정되어야 한다. 데이터보호담당관(data protection officer; DPO)은 컨트롤러에 의해 고용되었는지 여부와는 관계없이, 독립적으로 본인의 업무와 임무를 수행해야 한다.

(98) 컨트롤러 또는 프로세서의 범위를 대표하는 협회나 기타 기구는 이 법에서 정한 제한선에 따라 행동강령을 정하도록 권장되며, 이를 통해 특정분야에서 수행되는 처리의 구체적인 특성과 영세 및 중소기업의 구체적인 니즈(needs)를 고려하여 이 규정을 효과적으로 적용할 수 있게 된다. 특히, 이러한 행동강령은 처리가 개인의 권리와 자유에 초래할 수 있는 위험을 고려하여, 컨트롤러와 프로세서의 의무를 계산할 수 있다.

(99) 행동강령을 정할 때 또는 이러한 강령의 범위를 변경하거나 확대할 때, 컨트롤러 또는 프로세서의 범위를 대표하는 협회 또는 기타 기구들은, 가능한 경우 정보주체를 포함한 관련 이해관계자와 상의해야하며, 해당 자문에 대한 제출자료 및 견해를 참작해야 한다.

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

(101) 국제교역과 국제협력의 확대를 위해서는 유럽연합 역외국가 및 국제기구 간의 개인정보 이전이 필요하다. 개인정보의 국외이전의 증가로 인해 개인정보 보호와 관련한 새로운

과제 및 문제가 생겨났다. 그러나 개인정보가 유럽연합에서 제3국의 컨트롤러, 프로세서나 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 컨트롤러와 프로세서에게 개인정보가 재이전(onward transfer)되는 경우에도 동일하다. 어떤 경우에서도 제3국과 국제기구로의 정보 이전은 본 규정을 철저히 준수하여서만 시행될 수 있다. 개인정보 이전은 본 규정의 나머지 조문에 따라, 컨트롤러나 프로세서가 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 제3국이나 제3국의 영토 혹은 지정된(specified) 분야, 혹은 국제기관에서 적절한 수준이 개인정보보호를 보장하고 있다는 유효한 결정을, 유럽전체를 대신하여 내릴 수 있다. 따라서 유럽연합 전체는 이러한 보호수준을 보장한다고 간주되는 제3국이나 국제기관에 대해 법적 확실성과 균등성(uniformity)을 보장받을 수 있다. 이 경우, 해당 제3국이나 국제기관으로의 개인정보 이전은 추가적인 승인을 받을 필요 없이 진행될 수 있다. 또한 해당 제3국이나 국제기관에 사유를 설명하는 통지 및 성명서 전체를 전달한 후, 이러한 결정을 철회할 수 있다.

(104) 유럽연합 창설의 근거가 되는 인권보호 등의 기본적 가치에 따라, 집행위원회는, 제3국 또는 제3국의 영토나 규정된 분야에 대한 집행위원회의 평가에서, 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 지정된 분야에 대한 적정성 결정의 채택시에는 구체적인 정보처리 활동, 유효하고 적용 가능한 법적 기준 및 법률의 영역 등 해당 국가의 명확하고 객관적인 기준이 고려되어야 한다. 해당 제3국은 유럽연합 내에서 보장되는 수준에 상응하는 적정 수준의 개인정보 보호를 보장해야 한다. 이는 특히 개인정보가 하나 이상의 지정된 분야에서 처리될 경우 더욱 그러하다. 해당 제3국은 효과적이고 독립적인 개인정보보호 감독을 보장하고 회원국의 DPA와의 협력 메커니즘을 가능하게 해야 한다. 관련 정보주체는 효과적이고 행사 가능한 권리와 효과적인 행정적·사법적 구제방안을 제공받아야 한다.

(105) 제3국이나 국제기구가 체결한 국제협약과 별개로, 집행위원회는 해당 제3국이나 국제기구가 가입한 제도, 특히 개인정보 보호와 관련한 다자간·지역적 제도로부터 부여받은 의무 및 해당 의무의 이행을 고려해야 한다. 특히 1981년 1월 28일자 개인정보 자동처리 및 추가의정서에 대한 개인보호 유럽평의회 협약에 대한 제3국의 가입여부가 고려되어야 한다, 집행위원회는 제3국 또는 국제기구의 보호 수준을 평가 시, 각료이사회의 자문을 구해야 한다.

(106) 집행위원회는 제3국, 제3국내의 영토나 지정된 분야, 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 지정된 부문, 또는 국제기구가 더 이상 적정한 수준의 개인정보보호를 보장하지 않는다는 것을 인지할 수 있다. 이 경우, 구속력 있는 기업규칙(binding corporate rules) 등 적절한 안전장치에 근거하거나, 구체적 상황에 따른 적용제외(derogations)가 필요한 경우일 때를 제외하고는 해당 제3국이나 국제기구로의 개인정보 이전은 금지되어야 한다. 이 경우, 집행위원회와 해당 제3국이나 국제기구 간의 협의를 준비해야 한다. 집행위원회는 시기적절하게 관련 제3국이나 국제기구에 사유를 통보하고 상황 해결을 위한 협의에 들어가야 한다.

(108) 적정성 결정이 없을 경우, 컨트롤러나 프로세서는 정보주체를 위한 적절한 안전장치를 통해 제3국에서의 정보보호의 미흡함을 보완하기 위한 조치를 취해야 한다. 이 같은 적절한 안전장치로는 의무적 기업규칙(binding corporate rules), 집행위원회가 채택한 정보보호 표준조항(standard data protection clauses), 감독기관이 채택한 정보보호 표준조항 또는 감독기관이 승인한 계약조항(contractual clauses)을 활용할 수 있다. 이 같은 안전장치를 통해 유럽연합 역내의 정보처리에 적절한 개인정보 보호의 요건 및 정보주체의 권리가 보장되도록 해야 하며, 안전장치에는 유럽연합 및 제3국내에서 시행 가능한 정보주체의 권리의 가용조치, 효과적인 행정적, 사법적 구제 조치를 모색하고 보상을 요청하는 등, 효과적인 법적 구제를 위한 가용조치 등이 포함된다. 이러한 안전장치는 특히 개인정보처리에 관련된 일반적인 원칙, 데이터보호 설계 및 기본설정의 원칙을 준수해야 한다. MOU 등 행정협정에 삽입될 규정이 정보주체에 시행가능하고 효과적인 권리를 제공한다는 근거에 따라, 공공기관이나 공공기구는 제3국에 설립된 공공기관이나 공공기구 혹은 이에 상응하는 의무나 기능을 지닌 국제기관으로 정보를 이전할 수 있다. 법적 구속력이 없는 행정 협정에 안전장치가 제시될 경우 관련 감독기관의 승인이 필요하다.

(109) 컨트롤러나 프로세서가 집행위원회나 감독기관이 채택한 정보보호 표준조항을 활용한다면, 컨트롤러나 프로세서가 당해 프로세서와 기타 프로세서 간의 계약 등, 보다 광범위한 계약에 정보보호 표준조항을 포함시키는 것은 금지되어야 하며, 또는 집행위원회나 감독기관이 채택한 정보보호 표준조항이 직·간접적으로 위배하지 않고 정보주체의 기본권이나 자유를 침해하지 않는다고 하여, 기타 조항이나 추가적인 안전장치를 더해서는 안 된다. 컨트롤러와 프로세서는 정보보호 표준조항을 보완하는 계약적 의무를 통해 추가적인 안전장치를 제공하도록 독려되어야 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) 규제기구의 절차 등 사법절차, 행정적 또는 법원 이외의 다른 절차에 관계없이, 정보주체가 명백한 동의를 제공한 경우이거나 정보이전이 계약 혹은 법적 권리와 관련하여 간헐적이고 필요할 경우와 같이 특정한 상황에서 이루어질 수 있는 정보이전에 대한 조항을 규정해야 한다. 유럽연합 또는 회원국 법률에서 규정하고 있는 공익상의 이유로 요구될 수 있는 정보이전 혹은 법에 따라 설립되고 정당한 이익을 가진 대중 혹은 사람들의 조회 목적으로 기록부(register)로부터 정보이전이 이루어지는 경우에 대한 조항도 규정해야 한다. 후자의 정보이전 시, 개인정보 기록부(register)에 포함된 개인정보 전체 또는 정보 범주 전체를 포함해서는 안 된다. 그리고 개인정보 기록부(register)가 정당한 이익을 가진 사람의 조회용도일 때, 해당인의 요청에 한해서 혹은 그들이 수령인이 될 경우, 정보주체의 이익 및 기본권을 전적으로 고려하여 정보이전이 이루어져야 한다.

(112) 적용의 일부 제외는 특히 중요한 공익상의 이유로 요구되고 필요한 개인정보의 이전에 적용되어야 한다. 전자의 사례는 경쟁 당국, 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 특별 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 국제 인도주의 법률을 준수하기 위해 인도주의적 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 컨트롤러가 추구하는 정당한 이익보다 우선하지 않고, 컨트롤러가 개인정보 이전과 관련된 모든 정황을 평가한 후, 간헐적이고 한정된 숫자의 정보주체에 관한 정보이전은 컨트롤러가 추구하는 강력한 정당한 이익의 목적을 위해 가능할 수도 있다. 컨트롤러는 개인정보의 성격, 예정된 정보처리 작업(들)의 목적 및 지속기간, 개인정보 발송국가, 제3국 및 정보가 최종 이전되는 국가의 상황, 본인의 개인정보 처리와 관련해 개인의 기본권 및 자유를 보호하는데 적정한 안전장치를 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. 컨트롤러는 정보이전에 대하여 감독기관 및 해당 정보주체에 고지해야 한다.

(114) 어떤 경우에서도, 집행위원회가 제3국의 적정한 보호수준에 대해 아무런 결정을 내리지 않았을 경우, 컨트롤러나 프로세서는 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 자연인 및 법인의 개인정보 처리 활동을 직접 규제하기 위한 취지의 법률, 규정 및 기타 입법 기구를 채택한다. 여기에는 컨트롤러나 프로세서에게 개인정보의 이전이나 제공을 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 본 규정에 따른 제3국으로의 정보이전을 위한 조건을 만족시키는 경우에 한해서만 허용되어야 한다. 컨트롤러에 적용되는 유럽연합이나 회원국의 법률이 규정하는 공익상의 이유로 정보공개가 필요한 경우가 특히 이에 해당한다.

(116) 유럽연합 역외로의 개인정보 이전은 불법적인 개인정보 활용이나 제공으로부터 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 예방이나 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 감독기관의 단일 또는 복수의 위원에 대한 일반적 요건을 법률로 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 컨트롤러나 프로세서가 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 컨트롤러나 프로세서가 본인이 속한 국가에 거주하는 정보주체를 대상으로 시행하는 정보처리가 이에 해당한다. 정보주체가 제기한 민원처리, 본 규정 적용에 대한 조사 실시, 개인정보 처리와 관련한 위험, 규칙, 안전장치 및 권리에 대한 인식제고가 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 컨트롤러나 프로세서의 사업장의 활동 중 개인정보 처리가 이루어지거나, 컨트롤러나 프로세서가 하나 이상의 회원국에 설립된 경우, 혹은 유럽연합 역내의 컨트롤러나 프로세서의 단일 사업장의 활동 중 이루어진 정보처리가 하나 이상의 회원국 내 정보주체에 실질적으로 영향을 미치거나 그럴 가능성이 있는 경우, 해당 컨트롤러나 프로세서의 주 사업장 또는 단일 사업장을 관할하는 감독기관이 선임 감독기관이 된다. 선임 감독기관은 모든 관련 기관과 협력해야 한다, 그 이유는 관련 컨트롤러나 프로세서가 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 관련 감독기관이 되어야 한다. 이사회는 본 규정의 적용에 관한 질의사항에 대한 가이드라인을 발행하는 업무 중, 특히 해당 처리가 하나 이상의 회원국 내 정보주체에 실질적인 영향을 미쳤는지 여부를 확인하기 위해 고려해야 하는 기준에 대한 가이드라인과 유관하고 합리적인 이의에 필요한 요소에 대한 가이드라인을 특히 발행할 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, 컨트롤러나 프로세서의 주 사업장이나 단일 사업장을 대상으로 하며, 컨트롤러와 프로세서에 대해 구속력이 있어야 한다. 컨트롤러나 프로세서는 본 규정의 준수하기 위해 필요한 조치를 취하고, 유럽연합 내 개인정보 처리활동에 대해 컨트롤러나 프로세서의 주 사업장에 통보한 선임 감독기관의 결정을 이행하기 위해 필요한 조치를 취해야 한다.

(127) 선임 감독기관의 역할을 하지 않는 각 감독기관은, 컨트롤러나 프로세서가 하나 이상의 회원국에 설립된 경우, 해당 지역의 사안을 처리할 수 있어야 한다. 그러나 특정 정보처리의 대상은 단일 회원국 내에서 시행되는 처리에만 해당되고 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 또는 통보를 해온 감독기관이 지역 차원에서 해당 사안을 처리할 것인지 여부를 결정해야 한다. 자체적으로 해당 사안을 처리할 것인지 여부를 결정할 때, 선임 감독기관은 컨트롤러나 프로세서에 관한 결정을 효과적으로 이행하기 위해, 통보를 해온 감독기관이 속한 회원국에 컨트롤러나 프로세서의 사업장이 소재하고 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 고려되어야 한다.

(128) 선임 감독기관에 대한 규정 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 검찰 기관이 본 규정의 위반사건을 사법 기관에 제소하고 소송 절차에 관여할 권한을 침해해서는 아니 된다. 이 같은 권한에는 금지 등 정보처리를 임시적으로 또는 완전히 제한하는 권한도 포함된다. 회원국들은 본 규정에 의해 개인정보 보호와 관련된 기타 업무를 규정할 수 있다. 감독기관의 권한은 유럽연합 또는 회원국 법률에 제시된 적절한 절차의 안전장치에 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, 조

치를 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, 민원을 받은 감독기관의 견해를 최대한 고려해야 하며, 이 감독기관은 관할 감독기관과 연락하여, 자국의 영토에서 조사를 수행할 수 있는 권한을 여전히 가지고 있어야 한다.

(131) 제3의 감독기관이 컨트롤러나 프로세서의 정보처리 활동에 대한 선임 감독기관의 역할을 해야 하나, 민원의 구체적인 사안이나 위반 가능성이 민원을 제기 받거나 잠재적 침해 사고가 적발된 회원국의 컨트롤러나 프로세서의 정보처리 활동에만 관련이 있는 경우, 혹은 기타 회원국의 정보주체에 실질적인 영향을 미치지 않았거나 그럴 가능성이 없는 경우, 민원을 제기 받거나 적발되거나 혹은 본 규정에 대한 잠재적 위반가능성을 내포하는 상황을 다른 방식으로 통지 받은 감독기관은 컨트롤러와 원만한 합의를 보아야 하며, 이것이 성공적이지 못할 경우, 전범위의 권한을 행사해야 한다. 여기에는 감독기관이 소재한 회원국의 영토에서 시행되거나 그 회원국 영토의 정보주체에 관해 시행되는 특정한 개인정보 처리, 감독기구기 소재한 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) 대중을 대상으로 한 감독기관의 인식제고 활동에는 개인과 영세·중소기업 등의 컨트롤러와 프로세서를 겨냥한 구체적인 조치, 특히 교육적인 측면의 조치가 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, 유럽 데이터보호이사회(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, 유럽 데이터보호이사회는 협력 메커니즘 내에서 특히 본 규정의 위반 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 이행을 현저하게 방해할 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 적용이 의무인 경우, 이는 감독기관이 채택한 법적 효력을 발생시킬 목적의 조치의 적법성을 위한 하나의 조건이어야 한다. 국경을 넘는 처리와 관련이 있는 다른 경우에는, 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, 유럽 데이터보호이사회는 유럽연합의 독립기구로 설립되어야 한다. 목표 달성을 위해 유럽 데이터보호이사회는 법인격을 가져야 하고 의장이 유럽 데이터보호이사회를 대표해야 한다. 유럽 데이터보호이사회는 지침 95/46/EC이 제정한 개인정보 처리에 관한 개인보호 작업반을 대체해야 하고 각 회원국 감독기관의 장, 유럽 개인정보보호감독관(European Data Protection Supervisor) 또는 그에 상응하는 대표자로 구성되어야 한다. 집행위원회는 의결권 없이 유럽 데이터보호이사회의 활동에 참여하고 유럽개인정보보호 감독관은 특정 의결권을 보유해야 한다. 유럽 데이터보호이사회는 특히 제3국이나 국제기구의 보호 수준에 관하여 등 집행위원회에 자문을 제공하고 유럽연합 전역의 감독기관들의 협력을 도모함으로써 유럽연합 전역에 본 규정의 일관된 적용을 도와야 한다. 유럽 데이터보호이사회는 업무 수행 시 독립적으로 행동해야 한다.

(140) 유럽 데이터보호이사회는 유럽 개인정보보호감독관이 제공하는 사무처의 지원을 받아야 한다. 본 규정에 의해 유럽 데이터보호이사회에 부여된 업무를 수행하는 유럽 개인정보보호 감독관 직원들은 오로지 유럽 데이터보호이사회 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 민원의 절차 및 결과에 대해 정보주체에 통지해야 한다. 해당 사안이 추가 조사나 다른 감독기관과의 협력을 요구하는 경우, 정보주체는 중간 정보를

제공받아야 한다. 민원 제출을 용이하게 하기 위해, 각 감독기관은 기타 통신 수단을 배제하지 않고 전자적으로도 작성이 가능한 민원 제출 양식을 제공하는 등의 조치를 취해야 한다.

(142) 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 정보주체로부터의 권한 부여와 상관없이 자국 내에서 민원을 제기할 권리를 가지고, 정보주체의 권리가 본 규정을 침해하는 개인정보 처리로 인해 침해되었다고 간주할 사유가 있는 경우, 유효한 사법적 구제를 받을 권리를 가지도록 규정할 수 있다. 해당 기구, 단체나 협회는 정보주체로부터의 권한 부여와 상관없이 정보주체를 대신하여 보상을 청구하지 못할 수도 있다.

(143) 어떠한 개인 또는 법인이라도 유럽연합 기능에 관한 조약(TFEU) 제263조에 규정된 조건에 따라 유럽 데이터보호이사회의 결정을 취소하기 위해 사법재판소에 소송을 제기할 권리를 가진다. 이사회 결정의 수신대상으로서, 결정에 대해 이의를 제기하고자 하는 관련 감독기관들은 유럽연합 기능에 관한 조약(TFEU) 제263조에 따라 통지받은 후 두 달 이내에 소송을 제기하여야 한다. 유럽 데이터보호이사회의 결정이 컨트롤러, 프로세서나 민원인에게 직간접적으로 관련된 사안인 경우, 후자는 유럽연합 기능에 관한 조약(TFEU) 제263조에 따라 유럽 데이터보호이사회의 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. 이러한 결정은 특히 감독기관의 조사, 시정 및 인가 권한의 행사 또는 민원의 기각이나 거부와 관련 있다. 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, 유럽 데이터보호이사회의 결정을 이행하는 감독기관의 결정에 대해 국가 법정에 소가 제기되고 위원회의 결정의 타당성(유효성)이 문제가 되는 경우, 해당 국가의 법정은 위원회의 결정이 무효하다고 판결 내릴 권한은 없지만 그 결정이 무효하다고 간주되는 경우, 유럽연합 기능에 관한 조약(TFEU) 제267조에 따라 타당성의 문제를 사법재판소에 회부하여 사법재판소가 해석하도록 해야 한다. 그러나 특히 해당 결정에 직접적으로, 개인적으로

관련이 있었던 경우처럼 해당 결정의 취소를 위한 소를 제기할 기회가 있었으나 유럽연합 기능에 관한 조약(TFEU) 제263조가 규정한 기간 내에 그렇게 하지 못한 개인이나 법인의 요청인 경우, 회원국의 법정은 EU 데이터보호이사회의 결정의 타당성의 문제를 회부하지 않을 수 있다.

(144) 감독기관의 결정에 대한 소송 절차를 관장하는 법정은 동일한 컨트롤러나 프로세서에 의한 정보처리와 관련 있는 동일의 사안 등 동일한 개인정보 처리나 소송 사유에 관한 소송 절차에 대해 다른 회원국의 관련 법정에 소가 제기된다고 간주할 사유가 있다면, 이러한 관련 소송 절차의 여부를 확인하기 위해 해당 법정에 연락을 취해야 한다. 관련 소송 절차가 다른 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) 컨트롤러나 프로세서에 대한 소송 절차에서, 해당 컨트롤러가 공적 권한을 행사하는 회원국의 공공기관이 아니라면, 원고는 해당 컨트롤러나 프로세서가 사업장을 가지고 있거나 관련 정보주체가 거주하는 회원국의 법정에 소를 제기할 선택의 여지가 있어야 한다.

(146) 컨트롤러나 프로세서는 본 규정을 침해한 개인정보 처리의 결과로 개인이 감내해야 할지 모르는 피해 일체를 보상해야 한다. 컨트롤러나 프로세서는 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·시행 법률을 침해하는 개인정보 처리도 포함된다. 정보주체는 본인이 겪은 피해에 대해 전액의 실질적인 보상을 받아야 한다. 컨트롤러나 프로세서가 동일한 정보처리에 연루된 경우, 각 컨트롤러나 프로세서는 전체 피해에 대해 책임을 져야 한다. 그러나 그들이 동일한 소송 절차에 연결된 경우로, 피해를 입은 정보주체에게 전액의 실질적인 보상이 보장된다면, 회원국 법률에 의거하여, 해당 정보처리로 야기된 피해에 대한 각 컨트롤러나 프로세서의 책임에 따라 보상이 배분될 수 있다. 전액 보상을 지급한 컨트롤러나 프로세서는 차후 동일한 정보처리 건에 관련된 기타 컨트롤러나 프로세서들에 대해 상소 절차를 개시할 수 있다.

(147) 사법권에 대한 특정 규정이 본 규정에 포함되어 있는 경우로 특히 컨트롤러나 프로세서로부터의 보상 등의 사법적 구제를 모색하는 절차와 관련한 경우, 유럽 의회 및 각료이사회 규정서 (EU) No 1215/2012의 규정 등 일반적인 사법권의 규정이 상기의 특정 규정의 적용을 침해해서는 아니 된다.

(148) 본 규정서의 규정의 시행을 강화하기 위해, 본 규정에 따라 감독기관이 취한 적절한 조치에 더하거나 혹은 이를 대신하여 본 규정의 침해에 대한 행정 과태료 등 처벌이 부과되

어야 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 의도성, 피해 완화를 위해 취한 조치, 책임의 정도나 관련 침해행위의 전례 여부, 침해 사실이 감독기관에 통지된 방식, 컨트롤러나 프로세서에게 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 안전조치를 따라야 한다.

(149) 회원국들은 본 규정의 한도 내에서 채택된 국가 규정의 침해 등, 본 규정 침해에 대한 형사 처벌을 규정할 수 있어야 한다. 이러한 형사처벌에는 본 규정의 침해를 통해 얻은 이익의 박탈도 허용할 수 있어야 한다. 그러나 그 같은 국가 규정의 침해에 대한 형사처벌 및 행정 과태료의 부과가 사법재판소가 해석한 *일사부재리*의 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 사건별로, 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 침해로 인한 피해를 예방하거나 완화하기 위한 조치를 고려해야 한다. 행정 과태료가 한 사업체에 부과되는 경우, 사업체는 상기의 목적을 위해, 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 적용범위는 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 이러한 규정의 적용이 감독기관이 부과하는 행정 과태료에 상응하는 효력을 지닐 경우에 그러하다. 따라서 관할국의 법정은 과태료를 상정한 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. 관련 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 적용 제외 또는 면제를 받아야 한다. 이는 특히 시청각 분야 및 뉴스 아카이브와 언론 도서관에서의 개인정보 처리에 적용된다. 따라서 회원국은 이 같은 기본권 간의 균형을 유지시키려는 목적에 필요한 적용의 면제 및 일부 제외를 규정하는 입법적 조치를 채택해야 한다. 회원국은 통칙, 정보주체의 권리, 컨트롤러와 프로세서, 협력 및 일관성, 그리고 특정 정보처리 상황에 대해 이 같은 적용의 면제 및 일부 제외를 채택해야 한다. 회원국 간에 이 같은 면제 또는 일부 적용 제외가 상이한 경우, 컨트롤러가 따라야 하는 회원국의 법률이 적용되어야 한다. 모든 민주사회에서 표현의 자유권이 가지는 중요성을 고려하기 위해 저널리즘 등 자유에 관련된 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. 해당 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. 유럽 의회 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 해당 지침은 개인정보 보호를 근거로 열람 제도(access regime)에 의해 열람이 배제되거나 제한되는 문서 및 해당 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 고용 계약의 이행, 업무의 관리·계획·조직, 직장 내의 평등·다양성, 업무상의 건강·안전을 근거로 처리되고, 개별 또는 단체적 차원에서 고용과 관련한 권리 및 혜택을 행사하기 위한 목적으로 처리되며, 고용 관계의 종결을 목적으로 처리되는 조건을 규정할 수 있다.

(156) 공익상의 기록보존 목적, 과학적 또는 역사적 연구 목적 또는 통계적 목적의 개인정보 처리는 본 규정에 따른 정보주체의 권리와 자유를 위해 적절한 안전조치의 적용을 받아야 한다. 이러한 안전조치는 특히 데이터 최소화의 원칙을 보장하기 위해 기술적 및 관리적 조치가 마련되어 있도록 보장해야 한다. 공익상의 기록보존 목적, 과학적 또는 역사적 연구 목적 또는 통계적 목적의 추가적인 개인정보 처리는 (개인정보의 가명처리 등) 적절한 안전조치가 존재하는 경우로서, 컨트롤러가 정보주체를 식별할 수 없거나 더 이상 식별할 수 없는 개인정보를 처리하여 해당 목적을 충족시킬 가능성을 평가하였을 때 시행되어야 한다. 회원

국은 공익상의 기록보존 목적, 과학적 또는 역사적 연구 목적 또는 통계적 목적의 개인정보 처리를 위한 적절한 안전조치를 규정하여야 한다. 회원국은 특정 조건 하에서 정보주체를 위한 적절한 안전조치에 따라, 정보 제공에 관한 요건(information requirement) 및 공익상의 기록보존 목적, 과학적 또는 역사적 연구 목적 또는 통계적 목적으로 개인정보를 처리할 때 정정하고 삭제할 권리, 잊힐 권리, 정보를 이전하고 반대할 권리에 관한 세부사항 및 일부 적용제외 사항을 규정할 권한이 있어야 한다. 비례성 및 필요성의 원칙에 따라 개인정보의 처리를 최소화하려는 기술적 및 관리적 조치와 더불어, 특정 처리에서 추구하는 목적을 고려하여 적절한 경우, 정보주체가 상기의 권리를 행사하게 하기 위한 구체적인 절차가 이러한 조건과 안전조치에 포함되어 있을 수 있다. 과학적 목적으로의 개인정보 처리도 임상실험에 관한 법률 등 기타 관련 법률을 준수해야 한다.

(157) 연구원들은 기록부(registries)로부터의 정보를 연결하여, 심혈관계 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 지식 기반의 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) 기록보존의 목적으로 개인정보가 처리되는 경우, 본 규정이 망자에게는 적용되지 않아야 한다는 점을 유념하여 기록보존 목적의 정보처리에도 본 규정을 적용해야 한다. 공익을 위한 기록을 보유한 공공기관, 공공기구 또는 민간기구는, 유럽연합이나 회원국 법률에 따라, 일반적인 공익을 위해 지속적 가치가 있는 기록에 대한 접근(access)을 획득, 보존, 평가, 조성, 기술(describe), 통지, 장려(promote), 유포 및 제공할 법적 의무를 지닌 서비스를 지녀야 한다. 회원국은 예를 들어, 과거 전체주의 국가 체제 하의 정치적 행위, 집단 학살, 홀로코스트 등의 비인도적 범죄, 또는 전쟁 범죄에 관한 특정 정보를 제공할 목적으로, 유지·보존의 목적을 위한 개인정보의 추가적 처리를 규정할 권한을 위임 받아야 한다.

(159) 과학적 연구 목적으로 개인정보가 처리되는 경우, 본 규정은 해당 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 목적의 개인정보 공개(publication)나 다른 방식으로의 제공 등 특정 조건이 적용되어야 한다. 특히 보건 분야에서의 과학적 연구 결과가 정보주체의 이익을 위한 추가적 조치의 사유를 제공하는 경우, 이러한 조치를 고려하여 본 규정의 통칙이 적용되어야 한다.

(160) 역사적 연구 목적으로 개인정보가 처리되는 경우, 본 규정은 해당 정보처리에도 적용

되어야 한다. 여기에는 본 규정은 역사 연구 및 계보학 목적의 연구에도 포함되어야 하며, 망자에게는 적용되지 않는다는 점을 유념해야 한다.

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

(162) 통계 목적으로 개인정보가 처리되는 경우, 본 규정은 해당 정보처리에도 적용되어야 한다. 유럽연합 또는 회원국 법률은 본 규정의 한도 내에서 통계 내용, 접근(access) 통제, 통계 목적으로의 개인정보 처리에 대한 세부사항 및 정보주체의 권리와 자유를 보호하고 통계의 신뢰성을 보장하기 위한 적절한 조치를 결정해야 한다. 통계 목적이란 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 목적은, 통계 목적으로의 정보처리 결과가 개인정보가 아니라 총계 데이터 (aggregate data)이며, 이 결과나 개인정보는 어떠한 특정 개인에 관한 조치나 결정을 지지하는데 활용되지 않는다는 점을 함의하고 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. 유럽 의회 및 각료이사회 규정서 (EC) No 223/2009는 유럽연합 통계에 있어 통계의 신뢰성에 대한 추가 세부사항을 규정하고 있다.

(164) 감독기관이 컨트롤러나 프로세서로부터 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 규정되어 있듯이, 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 권한은 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 유럽 의회와 각료이사회로 전송되도록 해야 한다.

(167) 본 규정의 시행에 대한 균일한 조건을 보장하기 위해, 본 규정에서 규정하고 있는 경

우, 집행위원회에 시행 권한이 부여되어야 한다. 이 권한은 규정서 (EU) No 182/2011에 따라 행사되어야 한다. 이러한 정황에서 집행위원회는 영세기업과 중소기업을 위한 구체적인 조치를 고려해야 한다.

(168) 컨트롤러와 프로세서 간 및 프로세서 간에 체결된 표준계약조항·행동강령·기술표준 및 인증 메커니즘·제3국, 해당 제3국의 영토나 지정 부문, 또는 국제기구가 제공하는 적절한 보호수준· 정보보호표준조항·의무적 기업규칙에 대해 컨트롤러·프로세서·감독기관 간에 전자적 수단으로 정보를 교환하기 위한 양식과 절차, 상호지원, 감독기관 간, 그리고 감독기관과 EU 데이터보호이사회 간에 전자적 수단으로 정보를 교환하기 위한 방식(arrangements)에 대한 시행 법률을 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 시행 법률을 채택해야 한다.

(170) 유럽연합 전역에 동등한 개인의 보호수준 및 개인정보의 자유로운 이동을 보장하고자 하는 본 규정의 목적을 회원국이 충분히 달성할 수 없고, 조치의 규모나 효과의 이유로 유럽연합 차원에서 더 원활히 이 목적이 충족될 수 있으므로, 유럽연합은 유럽연합에 관한 협약(TEU) 제5조에 규정된 보완성의 원칙에 따른 조치를 채택할 수 있다. 동일한 조문에 규정된 비례성의 원칙에 따라, 본 규정은 그 목적을 충족시키는데 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, 정보주체가 동의를 제공한 방식이 본 규정의 조건에 부합하는 경우, 컨트롤러가 본 규정의 적용일 이후에 동일한 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) 유럽 개인정보보호감독관은 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 컨트롤러의 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 지침은 적절히 개정되어야 한다. 본 규정이 채택되는 대로, 특히 본 규정과의 일관성을 보장하기 위해 지침 2002/58/EC가 검토되어야 한다.

본 규정을 채택하였음:

개인정보의 처리와 관련한 개인의 보호 및 개인정보의 자유로운 이동에 관한 유럽의회와 유럽이사회 규정 (EU) No XXX/2016

제I장
일반 규정

제1조
주제 및 목적

1. 본 규정은 개인정보의 처리에 있어 자연인을 보호하기 위한 규칙과 개인정보의 자유로운 이동에 관한 규칙에 대하여 규정한다.

2. 본 규정은 자연인의 자유와 기본권, 특히 개인정보 보호에 대한 권리를 보호한다.

3. 유럽연합 내에서 개인정보의 자유로운 이동은, 개인정보를 처리함에 있어 자연인의 보호와 연관되어 있다는 이유로, 제한되거나 금지되어서는 안 된다.

제2조
물적 범위

1. 본 규정은 전적 또는 부분적으로 자동화 방식에 의해 이루어지는 개인정보의 처리와 자동화 수단 이외의 방식에 의한 것으로서 파일시스템을 구성하거나 구성하기 위한 개인정보의 처리에 적용된다.

2. 본 규정은 다음 각 호에 해당하는 개인정보의 처리에는 적용되지 않는다.

(a) 유럽연합 법률의 범위를 벗어나는 활동 중에 이루어지는 처리

(b) 회원국이 유럽연합 조약(TEU) 제5편, 제2장의 범위에 해당하는 활동을 수행할 때 이루어지는 처리

(c) 자연인이 순수하게 개인활동 또는 가정활동을 하는 중에 이루어지는 처리

(d) 공공의 안녕을 수호하고 이에 대한 위협을 예방하는 등 범죄의 예방, 조사, 적발, 기소 및 형벌 집행의 목적으로 관계당국에 의해 이루어지는 처리

3. 유럽연합 산하기관, 기구, 사무소 및 에이전시의 개인정보 처리에 대해서는 규정 45/2001/EC가 적용된다. 규정 45/2001/EC 및 그러한 개인정보의 처리에 적용 가능한 기타 유럽연합 법률은 제98조에 따라 본 규정의 원칙 및 규칙에 맞게 조정되어야 한다.

4. 본 규정은 지침 2000/31/EC의 적용, 특히 동 지침의 제12조부터 제15조까지에 규정된 중개서비스 사업자의 책임 규칙이 적용되는 것을 침해해서는 안 된다.

제3조
영토의 범위

1. 본 규정은 유럽연합 역내의 컨트롤러 또는 프로세서의 사업장의 활동에 수반되는 개인정보의 처리에 적용되고, 이 때 해당 처리가 유럽연합 역내 또는 역외에서 이루어지는지 여부는 관계없다.

2. 본 규정은 개인정보의 처리가 다음 각 호와 관련되는 경우, 유럽연합 역내에 설립되지 않은 컨트롤러 또는 프로세서가 유럽연합 역내에 거주하는 정보주체의 개인정보를 처리할 때도 적용된다.

(a) 정보주체가 지불을 해야 하는지에 관계없이 유럽연합 역내의 정보주체에게 재화와 용역을 제공

(b) 유럽연합 역내에서 발생하는 정보주체의 행태를 모니터링

3. 본 규정은 유럽연합 역내에 설립되지 않았으나 국제 공법에 의해 회원국의 법률이 적용되는 장소에 설립된 정보주체가 개인정보를 처리하는 데 적용된다.

제4조
정의

본 규정의 취지에 따르면

(1) 개인정보는 식별된 또는 식별 가능한 자연인('정보주체')과 관련한 일체의 정보를 가리킨다. 식별가능한 자연인은 직접 또는 간접적으로, 특히 이름, 식별번호, 위치정보, 온라인 식별자를 참조하거나 해당인의 신체적, 심리적, 유전적, 정신적, 경제적, 문화적 또는 사회적 정체성에 특이한 하나 이상의 요인을 참조함으로써 식별될 수 있는 자를 가리킨다.

(2) 처리는 자동화 수단에 의한 것인지 여부에 관계없이 단일의 또는 일련의 개인정보에 행해지는 단일 작업이나 일련의 작업으로서, 수집, 기록, 편집(organisation), 구성, 저장, 가공 또는 변경(adaptation or alteration), 검색(retrieval), 참조(consultation), 사용, 이전을 통한 제공, 배포나 기타 방식으로의 제공(dissemination or otherwise making available), 연동이나 연계(alignment or combination), 제한, 삭제 또는 파기 등이 이에 해당한다.

(3) 처리의 제한은 장래의 처리를 제한할 목적으로, 저장된 개인정보에 표시하는 행위를

의미한다.

(4) 프로파일링은 특히 자연인의 업무 성과, 경제적 상황, 건강, 개인적 선호, 관심사, 신뢰도, 행태, 위치 또는 이동에 관한 측면을 분석하거나 예측하기 위해 행해지는 경우로서, 자연인에 관련한 개인적인 특정 측면을 평가하기 위해 개인정보를 사용하여 이루어지는 모든 형태의 자동화된 개인정보의 처리를 가리킨다.

(5) 가명처리는 추가적인 정보의 사용 없이는 더 이상 특정 정보주체에게 연계될 수 없는 방식으로 개인정보를 처리하는 것이다. 단, 그 같은 추가 정보는 별도로 보관하고, 기술적 및 관리적 조치를 적용하여 해당 개인정보가 식별된 또는 식별될 수 있는 자연인에 연계되지 않도록 해야 한다.

(6) 파일링시스템은 기능적 또는 지리학적으로 중앙에 집중되거나 분산되었는지 여부에 관계없이 특정 기준에 따라 열람 가능한 일련의 구조화된 개인정보를 가리킨다.

(7) 컨트롤러는 단독으로 또는 제3자와 공동으로 개인정보 처리의 목적 및 방법을 결정하는 자연인 또는 법인, 공공기관, 기관, 기타 기구를 가리킨다. 그러한 처리의 목적 및 방법이 유럽연합 또는 회원국 법률로 결정되는 경우 컨트롤러 또는 컨트롤러자 지정을 위한 구체적 기준은 유럽연합 또는 회원국 법률로 규정될 수 있다.

(8) 프로세서는 컨트롤러를 대신하여 개인정보를 처리하는 자연인이나 법인, 공공기관, 기관 또는 기타 기구를 가리킨다.

(9) 수령인은 제3자 포함 여부에 관계없이 개인정보가 제공되는 자연인 또는 법인, 공공기관, 기관, 기타 기구를 가리킨다. 그러나 유럽연합 또는 회원국 법률에 따라 특정 조회업무를 수행하는 체제에서 개인정보를 수령할 수 있는 공공당국은 수령인으로 간주하지 않는다. 그러한 공공당국의 그 같은 개인정보의 처리는 처리 목적에 따라 적용 가능한 개인정보 보호 규칙을 준수하여야 한다.

(10) 제3자는 정보주체, 컨트롤러, 프로세서, 컨트롤러나 프로세서의 직권에 따라 개인정보를 처리할 수 있는 자를 제외한 자연인이나 법인, 공공기관, 기관 또는 기구를 가리킨다.

(11) 정보주체의 동의는 본인과 관련된 개인정보의 처리에 대해 합의한다는 정보주체의 희망을 진술 또는 명백한 적극적인 행위를 통해 자유롭고, 구체적으로, 결과에 대해 인지하여 분명하게 나타낸 의사표시를 가리킨다.

(12) 개인정보 침해는 이전 또는 저장되거나 기타 방식으로 처리된 개인정보가 우발적 또는 불법적으로 파기, 유실, 변경, 무단제공, 무단열람을 초래하게 되는 보안 위반을 가리킨다.

(13) 유전정보는 자연인의 생리나 건강에 관해 고유한 정보를 제공하는 해당인의 선천적 또는 후천적인 유전자 특성과 관련한 개인정보로서, 특히 해당 자연인의 생물학적 샘플 분석을 통해 획득하게 된다.

(14) 생체정보는 안면 영상이나 지문정보와 같이 특정 기술 처리로 얻어진 자연인의 신체적, 생리적, 행태적 특성과 관련된 정보로서, 자연인을 고유하게 식별할 수 있도록 해주거나 확인해주는 것을 의미한다.

(15) 건강에 관한 정보는 의료서비스 제공 등 자연인의 신체적 또는 정신적 건강과 관련한 개인정보를 가리키며, 해당인의 건강 상태에 관한 정보를 드러낸다.

(16) 주 사업장은 다음 각 호를 의미한다.

(a) 하나 이상의 유럽연합 회원국에 사업장을 운영하는 컨트롤러의 경우, 유럽연합 역내의 중앙 행정 지점을 주 사업장으로 본다. 유럽연합 역내의 또 다른 사업장에서 개인정보의 처리 목적 및 처리 방식을 결정하거나, 또 다른 사업장에서 개인정보의 처리 목적 및 처리 방식을 결정하게 할 집행권을 보유하고 있는 경우에는 또 다른 사업장을 주 사업장으로 본다.

(b) 하나 이상의 유럽연합 회원국에 사업장을 운영하는 프로세서의 경우, 유럽연합 역내의 중앙 행정 지점을 주 사업장으로 본다. 프로세서가 유럽연합 역내에 중앙 행정 지점을 가지고 있지 않은 경우에는, 프로세서에게 본 규정에 따른 특정 의무가 부과되는 범위 내에서 주요 처리 활동이 이루어지는 사업장을 주 사업장으로 본다.

(17) 대리인은 제27조에 따라 컨트롤러나 프로세서가 서면으로 지정하여 유럽연합 역내에 설립된 자연인 또는 법인으로서 본 규칙에 의거, 컨트롤러 또는 프로세서 각각의 의무에 대해 그들을 대신한다.

(18) 기업(enterprise)은 정례적으로 경제활동에 종사하는 합명회사, 조합 등 법적 형태와는 상관없이, 경제활동에 종사하는 자연인 또는 법인을 의미한다.

(19) 사업체 집단(group of undertakings)은 관리하는 사업체와 그 관리를 받는 사업체를 의미한다.

(20) 의무적 기업규칙(binding corporate rules)은 공동 경제활동에 종사하는 사업체 집단 또는 기업체 집단 내부에서 단일 또는 복수의 제3국에 위치한 컨트롤러나 프로세서에게 개인정보를 이전하기 위해, 유럽연합 회원국 영토에 설립된 컨트롤러 또는 프로세서가 준수하는 개인정보 정책을 의미한다.

(21) 감독기관(supervisory authority)은 제51조에 따라 유럽연합 회원국이 설립한 독립적인 공공기관을 의미한다.

(22) 관련 감독기관(supervisory authority concerned)은 다음 각 호의 사유로 개인정보 처리에 관여하는 감독기관을 의미한다.

(a) 해당 감독기관이 소재한 회원국의 영토에 컨트롤러나 프로세서가 설립되는 경우

(b) 해당 감독기관이 소재한 회원국에 거주하는 정보주체가 처리로 인해 상당한 영향을 받거나 받을 것으로 예상되는 경우

(c) 해당 감독기관에 민원이 제기된 경우

(23) 국가간 처리(cross-border processing)는 다음 각 호의 하나에 해당한다.

(a) 컨트롤러나 프로세서가 하나 이상의 회원국에 설립된 경우로서, 유럽연합 역내에 컨트롤러나 프로세서가 소재한 하나 이상의 회원국에서 사업장의 활동 중에 발생하는 개인정보의 처리
(b) 유럽연합 역내의 컨트롤러나 프로세서의 단일 사업장의 활동 중에 발생하지만 하나 이상의 회원국의 정보주체에게 상당한 영향을 미치거나 미칠 것으로 예상되는 개인정보의 처리

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

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

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

제II장
원칙

제5조
개인정보 처리 원칙

1. 개인정보는:

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

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

보지 않는다('목적 제한').

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

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

(e) 처리목적 달성에 필요한 기간 동안만 정보주체를 식별할 수 있는 형태로 보관되어야 한다. 개인정보는 제89조(1)에 따라 개인정보주체의 권리 및 자유를 보호하기 위해 본 규정이 요구하는 적절한 기술 및 관리적 조치를 시행하여 공익적 기록보존 목적, 과학적 또는 역사적 연구 목적, 통계적 목적을 위해 처리되는 경우 더 오랜 기간 동안 보관될 수 있다.

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

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

제6조
처리의 적법성

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

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

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

(c) 컨트롤러의 법적 의무를 준수하는데 개인정보 처리가 필요한 경우

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

(e) 공익을 위하거나 컨트롤러의 공식 권한을 행사하여 이루어지는 업무수행에 처리가 필요한 경우

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

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

2. 회원국은 본 규정의 규칙을 적용하기 위하여 더욱 구체적인 조문을 유지하거나 도입할 수 있다. 이는 개인정보 처리를 위한 구체적 요건과, 제IX장에서 규정하는 특정 처리 상황 등과 같이 적법하고 공정한 처리를 보장하기 위한 여타 조치들을 더욱 엄밀히 결정함으로써 제1항 (c)호 및 (e)호의 준수를 담보하기 위한 내용에 관한 것이다.

3. 제1항의 (c)호 및 (e)호에서의 개인정보 처리의 근거는 다음 각 호를 통해 규정되어야 한다.

(a) 유럽연합 법률

(b) 컨트롤러에게 적용되는 유럽연합 회원국의 법률

처리목적은 상기의 법적 근거에 의해 결정되어야 한다. 제1항 (e)호의 처리는 공익을 위하거나 컨트롤러의 공식권한을 행사하여 이루어지는 업무수행에 필요한 것이다. 해당 법적 근거로는 본 규정의 규칙을 적절히 적용하기 위한 특정 조문이 있을 수 있으며, 특히, 컨트롤러의 개인정보 처리 적법성에 대한 일반적인 조건, 해당 처리의 대상이 되는 개인정보의 유형, 관련 정보주체, 관련 개인정보의 제공 대상 및 목적, 목적 제한, 보관기간, 제IX장에서 규정하는 특정 처리상황을 위한 조치 등 합법적이고 공정한 처리를 보장하는 조치를 포함한 처리작업 및 처리절차가 이에 해당한다. 유럽연합 또는 회원국 법률은 공익의 목적을 달성하고 추구하는 적법한 목표에 비례해야 한다.

4. 개인정보를 수집한 목적 외로 처리하는 것이 정보주체의 동의 또는 제23조(1)의 목적을 보장하기 위한 민주사회의 필요하고 비례적인 조치를 구성하는 유렵연합 또는 회원국 법률에 근거하지 않는 경우, 컨트롤러는 개인정보의 목적 외 처리가 해당 개인정보를 수집한 당초 목적과 양립될 수 있는지 확인하기 위해서 특히 다음 각 호를 고려해야 한다.

(a) 수집 목적과 의도된 추가처리 목적 간의 연관성

(b) 특히 정보주체와 컨트롤러 간의 관계와 관련해서 등의 개인정보가 수집된 상황

(c) 특히 제9조에 따른 특정 범주의 개인정보가 처리되는지 여부 또는 제10조에 따른 범죄경력 및 범죄행위와 관련한 개인정보가 처리되는지 여부 등 개인정보의 성격

(d) 의도된 추가처리가 정보주체에 초래할 수 있는 결과

(e) 암호처리나 가명처리 등 적절한 안전조치의 존재

제7조
동의의 조건

처리가 동의를 기반으로 이루어지는 경우, 컨트롤러는 정보주체가 본인의 개인정보 처리에 동의하였음을 입증할 수 있어야 한다.

2. 정보주체의 동의가 기타의 사안과도 관련된 서면의 진술서로 제공되는 경우, 동의 요청은 그 기타의 사안과 분명히 구별되는 방식으로, 이해하기 쉽고 입수가 용이한 형태로, 명확하고 평이한 문구를 사용한 방식으로 제시되어야 한다. 진술서의 어느 부분이라도 본 규정을 위반하는 경우 그 구속력이 인정되지 않는다.

3. 정보주체는 언제든지 본인의 동의를 철회할 권리를 가진다. 동의의 철회는 철회 이전에 동의를 기반으로 한 처리의 적법성에 영향을 미치지 않는다. 정보주체는 동의를 제공하기 전에 이 사실에 대해 고지 받아야 한다. 동의의 철회는 동의의 제공만큼 용이해야 한다.

4. 동의가 자유롭게 제공되는지 여부를 평가할 때, 무엇보다 서비스 제공 등의 계약의 이행이 해당 계약의 이행에 필요하지 않은 개인정보의 처리에 대한 동의를 조건으로 하는지 여부를 최대한 고려해야 한다.

제8조
정보사회 서비스와 관련하여 아동의 동의에 적용되는 조건

1. 제6조(1)의 (a)호가 적용되는 경우, 아동에게 직접 이루어지는 정보사회서비스 제공과 관련하여 아동의 개인정보의 처리는 해당 아동이 최소 16세 이상인 경우에 적법하다. 아동이 16세 미만인 경우, 그 같은 처리는 해당 아동의 친권을 보유한 자가 동의를 제공하거나 승인한 경우에만 적법하다.

회원국은 상기의 목적에 대한 아동의 연령을 법률로서 낮추어 규정할 수 있으나, 해당 연령이 13세 미만이 되어서는 안 된다.

2. 그 같은 경우 컨트롤러는 가용한 기술을 고려하여 해당 아동의 친권을 보유한 자가 동의를 제공하거나 승인하였는지를 입증하기 위한 합당한 노력을 기울여야 한다.

3. 제1항은 아동과 관련한 계약의 유효성, 형식 또는 효력에 대한 규정 등 회원국의 일반 계약 법률에 영향을 미칠 수 없다.

제9조
특별 범주의 개인정보의 처리

1. 인종 또는 민족, 정치적 견해, 종교적 또는 철학적 신념, 노동조합의 가입여부를 나타내는 개인정보의 처리와 유전자 정보, 자연인을 고유하게 식별할 목적의 생체정보, 건강정보,

성생활 또는 성적 취향에 관한 정보의 처리는 금지된다.

2. 다음 각 호의 하나에 해당하는 경우 제1항은 적용되지 않는다.

(a) 정보주체가 단일 또는 복수의 특정한 목적으로 특별 범주의 개인정보를 처리하는 데 명백한 동의를 제공한 경우. 단, 유럽연합 또는 회원국 법률이 정보주체가 제1항의 금지조항을 무효화할 수 없다고 명시적으로 규정하는 경우는 제외된다.

(b) 고용, 사회보장, 사회보호법 분야에서 컨트롤러나 정보주체의 의무를 이행하고 특정 권리를 행사하기 위한 목적으로 처리가 필요한 경우. 단, 그 처리는 유럽연합 또는 회원국 법률이나 정보주체의 기본적 권리 및 이익에 대한 적절한 안전조치를 규정하는 회원국 법률에 따라 체결된 단체협약에 의해 승인되어야 한다.

(c) 정보주체가 신체적으로 또는 법률적으로 동의를 제공할 수 없는 경우로서 정보주체 또는 제3자의 생명의 이익을 보호하는 데 처리가 필요한 경우

(d) 정치적, 철학적, 종교적 또는 노동조합의 목적을 지닌 재단, 협회, 기타 비영리기관이 적절한 안전조치를 갖추어 수행하는 합법적인 활동의 과정에서 개인정보를 처리하는 경우로서, 해당 처리가 그 목적에 맞게 관련 기관의 회원 또는 이전 회원 또는 관련 기관과 정기적으로 접촉하는 자에 한하여 이루어지고, 정보주체의 동의 없이 이러한 개인정보를 기관 외부에 제공하지 않는다는 조건에 따라 수행되는 경우

(e) 정보주체가 명백히 공개한 개인정보와 관련된 처리인 경우

(f) 법적 권리의 확립, 행사, 방어를 위하거나 법원이 사법권을 행사할 때마다 처리가 필요한 경우

(g) 추구하는 목표에 비례하도록 유럽연합 또는 회원국 법률에 근거하여 상당한 공익상의 이유로 처리가 필요한 경우와 개인정보 보호권의 본질을 존중하고 정보주체의 기본적 권리 및 이익을 보호하기 위해 적절하고 구체적인 조치를 제공하는 경우

(h) 예방의학 또는 직업의학의 목적으로 처리가 필요한 경우 및 피고용인의 업무능력 평가, 의학적 진단, 의료서비스 또는 사회복지 또는 치료의 제공, 또는 유럽연합 또는 회원국 법률에 근거하거나 의료전문가와의 계약에 의거하고 제3항의 조건 및 안전조치에 따라 의료 또는 사회복지 제도나 서비스의 관리를 위해 처리가 필요한 경우

(i) 회원국 간의 중대한 건강 위협으로부터 보호하거나 의료서비스·의약품·의료장비의 높은 품질과 안정성을 보장하는 등 공중보건 분야에서 공익상의 이유로, 특히 직무상의 기밀 등 정보주체의 권리와 자유를 보호하기 위해 적절하고 구체적인 조치를 규정하는 유럽연합 또는 회원국 법률에 근거하여 처리가 필요한 경우

(j) 추구하는 목적에 비례하고, 개인정보 보호권의 본질을 존중하며, 정보주체의 기본적 권리

및 이익을 보호하기 위해 적절하고 구체적인 조치를 제공하는 유럽연합 또는 회원국 법률에 근거하여, 제89조(1)에 따라 공익적 기록보존 목적, 과학적 또는 역사적 연구 목적, 또는 통계적 목적을 위해 처리가 필요한 경우.

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

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

제10조

범죄경력 및 범죄행위에 관한 개인정보의 처리

범죄경력 및 범죄행위 또는 제6조(1)에 근거한 보안조치와 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 범죄경력 기록은 공공기관의 규제 하에서만 보관될 수 있다.

제11조

신원확인을 요하지 않는 개인정보의 처리

1. 컨트롤러가 개인정보를 처리하는 목적상 정보주체의 신원확인을 요구하지 않거나 더 이상 요구하지 않아도 되는 경우, 그 컨트롤러는 본 규정을 준수할 목적에 한하여 정보주체를 식별하기 위한 추가 정보를 유지, 취득, 처리할 의무를 가지지 않는다.

2. 본 조 제1항에 규정된 사례의 경우 컨트롤러가 정보주체를 식별할 수 없음을 입증할 수 있다면, 제15조부터 제20조까지의 조문은 적용되지 않는다. 단, 정보주체가 해당 조문에 따라 본인의 권리를 행사하기 위한 목적으로 본인의 신원을 확인할 수 있는 추가 정보를 제공하는 경우는 예외로 한다.

제ⅢⅢ장

정보주체의 권리

제1절

투명성 및 형식

제12조

정보주체의 권리 행사를 위한 투명한 정보, 통지 및 형식

1. 컨트롤러는 처리와 관련한 제13조 및 제14조에 명시된 일체의 정보, 제15조부터 제22조까지의 조문 및 제34조에 규정된 일체의 통지를 정확하고, 투명하며, 이해하기 쉬운 형식으로 명확하고 평이한 언어를 사용하여 정보주체에게 제공하기 위한 적절한 조치를 취해야 하고, 특히 아동을 특정 대상으로 할 때 더욱 그러해야 한다. 해당 정보는 서면이나 적절한 경우, 전자수단 등 기타 수단을 이용하여 제공되어야 한다. 정보주체가 요청하는 경우, 다른 수단을 통해 정보주체의 신원이 입증되면, 해당 정보는 구두로 제공될 수 있다.

2. 컨트롤러는 제15조부터 제22조까지의 조문에 따라 정보주체의 권리 행사를 용이하게 해야 한다. 제11조(2)의 경우에서 컨트롤러는 제15조부터 제22조까지의 조문에 따라 본인의 권리를 행사하려는 정보주체의 요청을 거절해서는 안 되며, 컨트롤러가 정보주체를 식별할 수 없음을 입증하는 경우는 예외로 한다.

3. 컨트롤러는 요청을 접수한 후, 한 달 이내에 부당한 지체 없이, 제15조에서 제22조까지의 조문에 따른 요청에 따라 취해진 조치에 대한 정보를 정보주체에게 제공해야 한다. 해당 요청의 복잡성과 요청 횟수를 참작하여 필요한 경우 해당 기간을 2개월 간 더 연장할 수 있다. 컨트롤러는 요청 접수 후 한 달 이내에 정보주체에게 기간 연장 및 지연 사유에 대해 고지하여야 한다. 정보주체가 전자양식의 수단으로 요청을 하는 경우, 정보주체로부터 별도의 요청이 있지 않는 한, 해당 정보는 가능한 전자양식으로 제공되어야 한다.

4. 컨트롤러가 정보주체의 요청에 대해 조치를 취하지 않는 경우, 정보주체에게 지체 없이 통지해야 하고 요청의 접수 후 최대 한 달 이내에 조치를 취하지 않은 사유 및 감독기관에 민원을 제기하고 사법 구제를 받을 수 있는 가능성에 대해 정보주체에게 고지해야 한다.

5. 제13조 및 제14조에 명시된 정보와 제15조부터 제22조까지의 조문 및 제34조에 따른 일체의 통지와 조치는 무상으로 제공되어야 한다. 정보주체의 요청이 명백하게 근거가 없거나 과도한 경우, 특히 요청이 반복될 경우, 컨트롤러는 다음 각 호의 하나에 따를 수 있다.

(a) 관련 정보 또는 통지를 제공하거나 요청한 조치를 취하는 데 소요되는 행정적 비용을 참작하여 합리적인 비용을 부과한다.

(b) 해당 요청에 대한 응대를 거부한다.

컨트롤러는 해당 요청이 명백하게 근거가 없거나 과도하다는 사실을 입증할 책임이 있다.

6. 제15조에서 제19조까지의 조문에 규정된 요청을 하는 개인의 신원과 관련하여 합리적인 의심이 드는 경우, 컨트롤러는 제11조를 침해하지 않고 정보주체의 신원을 확인하는 데 필요한 추가적 정보 제공을 요청할 수 있다.

7. 제13조 및 제14조에 따라 정보주체에게 제공되는 정보는 예정된 처리에 대해 유의미한 개요를 제공하고자 표준화된 아이콘과 결합하여 가시적이고 이해하기 쉬우며 가독성이 뛰어난 방식으로 제공될 수 있다. 해당 아이콘이 전자 방식으로 제공되는 경우, 이는 기계 판독이 가능해야 한다.

8. 집행위원회는 아이콘으로 제시되는 정보 및 표준 아이콘의 제공 절차를 결정하기 위한 목적으로 제92조에 따라 위임 법률을 채택할 권한을 갖는다.

제2절
정보 및 개인정보 열람

제13조
개인정보가 정보주체로부터 수집되는 경우 제공되는 정보

1. 정보주체에 관련된 개인정보를 정보주체로부터 수집하는 경우, 컨트롤러는 개인정보를 취득할 당시 정보주체에게 다음 각 호의 정보 일체를 제공해야 한다.

(a) 컨트롤러 또는 해당되는 경우, 컨트롤러의 대리인의 신원 및 상세 연락처

(b) 해당되는 경우, 데이터보호담당관의 상세 연락처

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

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

(e) 해당되는 경우, 개인정보의 수령인 또는 수령인의 범주

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

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

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

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

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

(d) 감독기관에 민원을 제기할 수 있는 권리

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

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

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

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

제14조

개인정보가 정보주체로부터 수집되지 않은 경우 제공되는 정보

1. 개인정보가 정보주체로부터 수집되지 않은 경우, 컨트롤러는 다음 각 호의 정보를 정보주체에게 제공해야 한다.

(a) 컨트롤러 또는 가능한 경우, 컨트롤러의 대리인의 신원 및 상세 연락처

(b) 해당되는 경우, 데이터보호담당관의 상세 연락처

(c) 해당 개인정보의 예정된 처리 목적뿐 아니라 처리의 법적 근거

(d) 관련 개인정보의 범주

(e) 해당되는 경우, 개인정보의 수령인 또는 수령인의 범주

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

2. 제1항의 정보와 함께, 컨트롤러는 정보주체와 관련한 공정하고 투명한 처리를 보장하는 데 필요한, 다음 각 호의 정보를 정보주체에 제공해야 한다.

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

(b) 제6조(1)의 (f)호에 근거한 처리의 경우, 컨트롤러 또는 제3자의 정당한 이익

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

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

(e) 감독기관에 민원을 제기할 수 있는 권리

(f) 개인정보의 출처, 가능한 경우 해당 개인정보가 공개 출처로부터 비롯되었는지 여부

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

3. 컨트롤러는 제1항 및 제2항에 명시된 정보를 다음 각 호와 같이 제공해야 한다.

(a) 개인정보가 처리된 특정 상황과 관련하여 개인정보를 입수한 후 최소 한 달 이내의 합리적인 기간 내

(b) 개인정보가 정보주체에게 통지할 목적으로 사용되는 경우, 최소한 해당 정보주체에

최초로 통지한 시점

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

4. 컨트롤러가 수집 목적 이외의 목적으로 개인정보를 추가 처리하려는 경우, 해당 컨트롤러는 추가 처리 이전에 정보주체에게 해당되는 기타의 목적에 대한 정보와 제2항에 규정된 관련 추가 정보의 일체를 제공해야 한다.

5. 다음 각 호에 해당하는 경우 그 범위에 한하여 제1항부터 제4항까지가 적용되지 않는다.

(a) 정보주체가 이미 해당 정보를 보유하고 있는 경우

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

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

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

제15조

정보주체의 열람권

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

(a) 처리 목적

(b) 관련된 개인정보의 범주

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

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

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

(f) 감독기관에 민원을 제기할 수 있는 권리

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

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

2. 개인정보가 제3국이나 국제기구로 이전되는 경우, 정보주체는 제46조에 따라 적절한 안전조치에 대해 고지 받을 권리가 있다.

3. 컨트롤러는 처리가 진행 중인 개인정보의 사본을 제공해야 한다. 정보주체가 추가 사본을 요청하는 경우, 컨트롤러는 행정적 비용에 근거하여 합리적인 비용을 청구할 수 있다. 정보주체가 전자적 방식으로 해당 요청을 하는 경우, 관련 정보는 통상적으로 사용되는 전자적 양식으로 제공되어야 한다.

4. 제3항에 규정된 사본을 입수할 권리는 제3자의 권리와 자유를 침해하지 않아야 한다.

제3절
정정 및 삭제

제16조
정정권

정보주체는 본인에 관하여 부정확한 개인정보를 부당한 지체 없이 정정하도록 컨트롤러에게 요구할 권리를 가진다. 정보주체는 처리목적을 참작하여 추가 진술을 제공할 수단을 통하는 등, 불완전한 개인정보를 보완할 권리를 가진다.

제17조
삭제권('잊힐 권리')

1. 정보주체는 본인에 관한 개인정보를 부당한 지체 없이 삭제하도록 컨트롤러에게 요청할 권리를 가지며, 컨트롤러는 다음 각 호가 적용되는 경우, 부당한 지체 없이 개인정보를 삭제할 의무를 가진다.

(a) 개인정보가 수집된, 그렇지 않으면 처리된 목적에 더 이상 필요하지 않은 경우

(b) 정보주체가 제6조(1)의 (a)호 또는 제9조(2)의 (a)호에 따라 처리의 기반이 되는 동의를 철회하고, 해당 처리에 대한 기타의 법적 근거가 없는 경우

(c) 정보주체가 제21조(1)에 따라 처리에 반대하고 관련 처리에 대해 우선하는 정당한 근거가 없거나, 정보주체가 제21조(2)에 따라 처리에 반대하는 경우

(d) 개인정보가 불법적으로 처리된 경우

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

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

2. 컨트롤러가 개인정보를 공개하고 제1항에 따라 해당 개인정보를 삭제할 의무가 있는 경우, 컨트롤러는 가용 기술과 시행 비용을 참작하여 개인정보를 처리하는 컨트롤러에게 정보주체가 그 같은 컨트롤러들에게 해당 개인정보에 대한 링크, 사본 또는 복제본의 삭제를 요청하였음을 고지하기 위한 기술적 조치 등, 적절한 조치를 취해야 한다.

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

(a) 표현과 정보의 자유에 대한 권리의 행사

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

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

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

(e) 법적 권리의 확립, 행사 또는 방어를 위한 경우

제18조

처리에 대한 제한권

1. 다음 각 호의 하나에 해당하는 경우, 정보주체는 컨트롤러로부터 처리의 제한을 얻을 권리를 가진다.

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

(d) 컨트롤러의 정당한 이익이 정보주체의 정당한 이익에 우선하는지 여부를 확인할 때까지, 정보주체가 제21조(1)에 따라 처리에 대해 반대하는 경우

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

3. 제1항에 따라 처리의 제한을 취득한 정보주체는 처리제한이 해제되기 전에 컨트롤러로부터 이를 고지 받아야 한다.

제19조

개인정보의 정정이나 삭제 또는 처리의 제한에 관한 고지 의무

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

제20조

개인정보 이동권

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

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

(b) 처리가 자동화된 수단으로 시행되는 경우

2. 제1항에 따른 본인의 개인정보 이동권을 행사하는 데 있어, 정보주체는 기술적으로 가능한 경우 해당 개인정보를 한 컨트롤러에서 다른 컨트롤러로 직접 이전할 권리를 가진다.

3. 본 조 제1항에 규정된 권리의 행사는 제17조를 침해해서는 안 된다. 해당 권리는 공익을 위해서 또는 컨트롤러에게 부여된 공식권한을 행사하여 이루어지는 업무 수행에 필요한 처리에는 적용되지 않는다.

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

제4절
반대할 권리 및 자동화된 개별 의사결정

제21조
반대할 권리

1. 정보주체는 본인의 특별한 상황에 따라 제6조(1)의 (e)호 및 (f)호에 근거한 프로파일링 등, 본인과 관련한 개인정보의 처리에 대해 언제든지 반대할 권리를 가진다. 컨트롤러는 정보주체의 이익, 권리 및 자유에 우선하는 처리를 위한, 또는 법적 권리의 확립, 행사나 방어를 위한 설득력 있는 정당한 이익을 입증하지 않는 한, 해당 개인정보를 더 이상 처리해서는 안 된다.

2. 직접 마케팅을 목적으로 개인정보가 처리되는 경우, 정보주체는 언제든지 해당 마케팅을 위한 본인에 관한 개인정보의 처리에 반대할 권리가 있으며, 그러한 처리에는 해당 직접 마케팅과 관련된 경우 프로파일링이 포함된다.

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

4. 제1항 및 제2항의 권리는, 아무리 늦어도 정보주체에게 처음 고지한 시점에, 명백하게

정보주체에게 통지되어야 하며, 명확하고 기타 정보와는 별도로 제공되어야 한다.

5. 정보사회서비스 이용의 환경에서, 또한 지침 2002/58/EC에 관계없이, 정보주체는 기술 규격서를 사용한 자동화된 수단을 통해 반대할 권리를 행사할 수 있다.

6. 개인정보가 제89조(1)에 의거한 과학적 또는 역사적 연구 목적이나 통계적 목적을 위해 처리되는 경우로서, 공익을 위한 업무 수행에 필요한 처리가 아닌 경우라면 정보주체는 본인과 관련한 특별한 상황에 따라 본인에 관한 개인정보의 처리에 반대할 권리를 가진다.

제22조

프로파일링 등 자동화된 개별 의사결정

1. 정보주체는 프로파일링 등, 본인에 관한 법적 효력을 초래하거나 이와 유사하게 본인에게 중대한 영향을 미치는 자동화된 처리에만 의존하는 결정의 적용을 받지 않을 권리를 가진다.

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

(a) 정보주체와 컨트롤러 간의 계약을 체결 또는 이행하는 데 필요한 경우

(b) 컨트롤러에 적용되며, 정보주체의 권리와 자유 및 정당한 이익을 보호하기 위한 적절한 조치를 규정하는 유럽연합 또는 회원국 법률이 허용하는 경우

(c) 정보주체의 명백한 동의에 근거하는 경우

3. 제2항 (a)호 및 (c)호의 사례의 경우, 컨트롤러는 정보주체의 권리와 자유 및 정당한 이익, 최소한 컨트롤러의 인적 개입을 확보하고 본인의 관점을 피력하며 결정에 대해 이의를 제기할 수 있는 권리를 보호하는 데 적절한 조치를 시행해야 한다.

4. 제2항의 결정은 제9조(2)의 (a)호와 (g)호가 적용되고, 정보주체의 권리와 자유 및 정당한 이익을 보호하는 적절한 조치가 갖추어진 경우가 아니라면 제9조(1)의 특별 범주의 개인정보를 근거로 해서는 안 된다.

제5절

제한

제23조

제한

1. 컨트롤러나 프로세서에게 적용되는 유럽연합 또는 회원국 법률은 입법 조치를 통해 제5조뿐만 아니라 제12조부터 제22조까지의 조문과 제34조에 규정된 의무 및 권리의 영역을 제한할 수 있다. 단, 그러한 제한이 기본적 권리 및 자유의 본질을 존중하고 민주사회에서 다음 각 호를 보호하는 데 필요하고 비례적인 조치일 때로 유럽연합 또는 회원국 법률의 조문이 제12조부터 제22조까지의 조문에 규정된 권리 및 의무에 상응하는 경우에 그러하다.

(a) 국가안보

(b) 국방

(c) 공공 안보(public security)

(d) 공안의 보호 및 공안에 대한 위협의 예방 등 범죄의 예방, 수사, 적발, 또는 형사범죄의 기소나 형벌의 집행

(e) 유럽연합 또는 회원국의 일반적 공익을 위한 기타 중요한 목표로서, 특히 통화, 예산, 과세 현안, 공중보건 및 사회보장 등, 유럽연합 또는 회원국의 중요한 경제적 또는 재정적 이익

(f) 사법 독립성 및 사법 절차에 대한 보호

(g) 규제대상 직종(regulated professions)의 윤리 침해에 대한 예방, 조사, 적발, 기소

(h) (a), (b), (c), (d), (e), (g)호에서 규정된 경우, 부정기적일지라도 공적 권한의 행사와 연계된 모니터링, 점검, 또는 규제기능

(i) 정보주체 또는 제3자의 권리와 자유에 대한 보호

(j) 민법 청구의 집행

2. 특히, 제1항의 모든 입법 조치에는 관련이 있는 경우 최소한 다음 각 호에 관한 구체적인 조문이 포함되어야 한다.

(a) 처리 또는 처리 범주의 목적

(b) 개인정보의 범주

(c) 도입된 제한의 범위

(d) 남용, 불법 열람 또는 이전을 예방하기 위한 안전조치

(e) 컨트롤러나 컨트롤러 범주에 대한 상세설명

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

(g) 정보주체의 권리 및 자유에 대한 위험

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

제IV장

컨트롤러와 프로세서

제1절

일반적 의무

제24조

컨트롤러의 책임

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

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

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

제25조

설계 및 기본설정에 의한 개인정보 보호

1. 컨트롤러는 개인정보의 처리가 자연인의 권리 및 자유에 미치는 위험의 다양한 가능성 및 정도와 함께 최신 기술, 실행 비용, 그리고 처리의 성격, 범위, 상황 및 목적을 고려하여, 가명처리 등의 기술 및 관리적 조치를 개인정보의 처리 방법을 결정한 시점 및 그 처리가

이루어지는 해당 시점에 이행해야 한다. 그러한 기술적 및 관리적 조치는 본 규정의 요건을 충족시키고 정보주체의 권리를 보호하기 위해 데이터 최소화 등 개인정보 보호원칙을 효율적으로 이행하고 필요한 안전조치를 개인정보 처리에 통합할 수 있도록 설계되어야 한다.

2. 컨트롤러는 기본설정을 통해 각 특정 처리 목적에 필요한 개인정보만 처리되도록 적절한 기술적 및 관리적 조치를 이행해야 한다. 그 의무는 수집되는 개인정보의 양, 그 처리 정도, 보관기관 및 이용가능성에 적용된다. 특히, 그러한 조치는 기본설정을 통해 개인정보가 관련 개인의 개입 없이 불특정 다수에게 열람되지 않도록 한다.

3. 제42조에 의거한 승인된 인증 메커니즘은 본 조 제1항 및 제2항에 규정된 요건의 준수를 입증하는 요소로 사용될 수 있다.

제26조

공동 컨트롤러

1. 두 명 이상의 컨트롤러가 공동으로 처리의 목적과 방법을 결정하는 경우, 이들은 공동 컨트롤러가 된다. 공동 컨트롤러는 당사자 간의 협의를 통해, 본 규정에 따른 책임을 준용, 특히 정보주체의 권리 행사에 대한 각자의 책임과 제13조 및 제14조의 정보를 제공할 각자의 임무를 투명하게 결정해야 하되, 그러한 각자의 책임이 컨트롤러에 적용되는 유럽연합 또는 회원국 법률에 의해 결정되는 경우는 예외로 한다. 그러한 협의를 통해 정보주체에 대한 연락담당관을 지정할 수 있다.

2. 제1항의 협의는 정보주체에 대한 공동 컨트롤러의 개별 역할과 관계를 충분히 반영해야 한다. 해당 협의의 골자를 정보주체에 제공해야 한다.

3. 제1항의 협의의 조건과 관계없이, 정보주체는 본 규정에 따라 각 컨트롤러와 관련하여, 그리고 이들에 반대하여 본인의 권리를 행사할 수 있다.

제27조

유럽연합 내에 설립되지 않은 컨트롤러 또는 프로세서의 대리인

1. 제3조(2)가 적용되는 경우, 컨트롤러 또는 프로세서는 유럽연합 역내 대리인을 서면으로 지정해야 한다.

2. 이 의무는 다음 각 호에 적용되지 않는다.

(a) 부정기적인 처리로서, 제9조(1)의 특별 범주의 개인정보의 처리 또는 제10조의 범죄경력

및 범죄행위에 관한 개인정보의 처리가 대규모로 이루어지지 않으며, 처리의 성격, 정황, 범위 및 목적을 고려할 시 자연인의 권리 및 자유에 위험을 초래할 가능성이 없는 경우

(b) 공공당국 또는 기관

3. 대리인은 정보주체가 거주하고, 재화 또는 용역의 제공과 관련하여 해당 정보주체의 개인정보가 처리되거나 행동이 모니터링 되는 회원국 중 한 곳에 설립되어야 한다.

4. 대리인은 컨트롤러 또는 프로세서에 의해 위임되며, 컨트롤러 또는 프로세서와 함께, 또는 이들을 대신하여 본 규정을 준수하기 위한 목적으로 처리와 관련한 모든 사안에 대해 감독기관 및 정보주체와 교섭해야 한다.

5. 컨트롤러 또는 프로세서의 대리인 지정은 컨트롤러 또는 프로세서 본인에게 제기될 수 있는 법적 조치를 침해하지 않아야 한다.

제28조

프로세서

1. 컨트롤러를 대신하여 처리가 이루어지는 경우, 컨트롤러는 적절한 기술 및 관리적 조치 이행을 통해 그 처리가 본 규정의 요건을 충족시키고, 정보주체의 권리를 보호하도록 충분한 보증을 제공하는 프로세서만 이용해야 한다.

2. 프로세서는 사전의 특정한 또는 일반적인 컨트롤러의 서면 승인 없이 타 프로세서를 고용할 수 없다. 일반적인 서면 승인의 경우, 프로세서는 컨트롤러에게 타 프로세서의 추가 또는 대체와 관련한 예정된 변경에 대해 고지하여, 컨트롤러가 이러한 변경에 반대할 기회를 제공해야 한다.

3. 프로세서의 처리는 컨트롤러와 관련하여 프로세서에게 구속력을 가지고, 처리의 주제와 지속기간, 처리의 성격과 목적, 개인정보의 유형과 정보주체의 범주, 컨트롤러의 의무와 권리를 규정하는 유럽연합 또는 회원국 법률에 따른 계약이나 기타 법률의 규제를 받는다. 그 계약 또는 기타 법률은 프로세서에 대하여 특히 다음 각 호와 같이 규정해야 한다.

(a) 프로세서는 컨트롤러의 서면 지시에 한하여 개인정보를 처리하며, 여기에는 제3국 또는 국제기구로의 개인정보 이전이 포함되며, 유럽연합 또는 프로세서에 적용되는 회원국 법률이 요구하는 경우는 제외한다. 이 경우, 프로세서는 처리 이전에 해당 법률요건을 컨트롤러에게 고지해야 하며, 해당 법률이 공익상의 중요한 이유로 그러한 통지를 금지하는 경우는 예외로 한다. 제3국 또는 국제기구로의 개인정보 이전에 관해서 등 컨트롤러의 문서화된 지시에 한하여 개인정보를 처리하나, 프로세서에게 적용되는 유럽연합 또는 회원국 법률로 요구되는 경우는 제외한다.

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

(c) 제32조에 따라 요구되는 모든 조치를 취한다.

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

(e) 해당 처리의 성격을 참작하여, 제Ⅲ장에 규정된 정보주체의 권리행사의 요청에 대응해야 하는 컨트롤러의 의무 이행을 위해, 가능한 경우, 적절한 기술적 및 관리적 조치를 통해 컨트롤러를 지원한다.

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

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

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

(h)호와 관련하여, 프로세서는 어떠한 지시가 본 규정 또는 기타 유럽연합 또는 회원국의 개인정보 보호 조문을 위반한다고 판단되는 경우 즉시 컨트롤러에게 이에 대해 통지해야 한다.

4. 프로세서가 컨트롤러를 대신하여 특정 처리 활동을 수행하기 위해 타 프로세서와 함께 일하는 경우, 제3항에 규정된 컨트롤러와 프로세서 간의 계약 또는 기타 법률에 명시된 동일한 개인정보 보호의 의무는 유럽연합 또는 회원국 법률에 따른 계약이나 기타 법률의 방식으로 관련 타 프로세서에게 부과되어야 하며, 특히 해당 처리가 본 규정의 요건을 충족시키는 방식으로 적절한 기술적 및 관리적 조치를 이행하는 것에 대해 충분한 보증을 제공해야 한다. 해당 타 프로세서가 본인의 개인정보 보호의 의무를 이행하지 않을 경우, 최초의 프로세서는 그 프로세서의 의무 이행에 대해 컨트롤러에게 전적인 책임을 져야 한다.

5. 프로세서가 제40조의 승인된 행동강령 또는 제42조의 공인 인증 메커니즘을 준수하는 것은 본 조 제1항 및 제4항에 규정된 충분한 보증을 입증하는 요소로 활용될 수 있다.

6. 컨트롤러와 프로세서 간의 개별 계약을 침해하지 않고, 본 조 제3항 및 제4항에 규정된 계약 또는 기타 법률은 전적 또는 부분적으로 본 조 제7항 및 제8항에 규정된 정보보호 표준 계약조항(standard contractual clauses)에 근거할 수 있으며, 해당 계약 및 기타 법률이 제42조 및 제43조에 따라 컨트롤러 또는 프로세서에게 수여된 인증의 일부인

경우에도 그러하다.

7. 집행위원회는 본 조 제3항 및 제4항에 규정된 사안에 대하여, 제93조(2)에 규정된 심사 절차에 따라 정보보호 표준 계약조항을 규정할 수 있다.

8. 감독기관은 본 조 제3항 및 제4항에 규정된 사안에 대하여, 제63조에 규정된 일관성 메커니즘에 따라 정보보호 표준 계약조항을 채택할 수 있다.

9. 제3항 및 제4항에 규정된 계약이나 기타 법률은 전자 양식 등 서면으로 작성되어야 한다.

10. 제82조, 제83조, 제84조를 침해하지 않고, 프로세서가 처리의 목적 및 방법을 결정함으로써 본 규정을 위반하는 경우, 프로세서는 해당 처리와 관련하여 컨트롤러로 간주되어야 한다.

제29조

컨트롤러 및 프로세서의 권한에 따른 처리

프로세서, 그리고 컨트롤러나 프로세서의 권한에 따라 행하는 자로서 개인정보를 열람할 수 있는 자는 유럽연합 또는 회원국 법률로 요구되는 경우가 아니라면 컨트롤러의 지시에 따른 경우를 제외하고 해당 개인정보를 처리해서는 안 된다.

제30조

처리 활동의 기록

1. 각 컨트롤러와, 해당하는 경우, 그 컨트롤러의 대리인은 본인의 책임 하에 진행되는 처리 활동의 기록을 보존해야 한다. 해당 기록은 다음 각 호의 정보를 포함해야 한다.

(a) 컨트롤러와, 해당하는 경우, 공동 컨트롤러, 컨트롤러의 대리인 및 데이터보호담당관의 이름 및 연락처

(b) 처리의 목적

(c) 정보주체의 범주 및 개인정보의 범주에 대한 설명

(d) 제3국 또는 국제기구의 수령인 등, 개인정보를 제공받았거나 제공받을 예정인 수령인의 범주

(e) 해당하는 경우, 제3국 및 국제기구의 신원 확인 등, 제3국 또는 국제기구로의 개인정보 이전 및 제49조(1)의 2호에 규정된 이전의 경우에는 적절한 안전조치에 대한 문서

(f) 가능한 경우, 각기 다른 범주의 정보를 삭제하는 데 예상되는 기한

(g) 가능한 경우, 제32조(1)에 규정된 기술 및 관리적 안전조치에 대한 전반적인 설명

2. 각 프로세서, 그리고 해당하는 경우 관련 프로세서의 대리인은 컨트롤러를 대신하여 수행하는 전 범주의 처리활동에 대한 기록을 보존해야 하며, 해당 기록은 다음 각 호의 정보를 포함해야 한다.

(a) 관련 프로세서(들) 및 프로세서가 대행하는 각 컨트롤러의 이름과 연락처, 그리고 해당하는 경우, 컨트롤러와 프로세서의 대리인 및 데이터보호담당관의 이름과 연락처

(b) 각 컨트롤러를 대신하여 수행하는 처리의 범주

(c) 해당하는 경우, 제3국 및 국제기구의 신원 확인 등, 제3국 또는 국제기구로의 개인정보 이전 및 제49조(1)의 2호에 규정된 이전의 경우에는 적절한 안전조치에 대한 문서

(d) 가능한 경우, 제32조(1)에 규정된 기술 및 관리적 안전조치에 대한 전반적인 설명

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

4. 해당 컨트롤러와 프로세서, 그리고 해당하는 경우, 컨트롤러 또는 프로세서의 대리인은 요청이 있을 경우 감독기관에 기록을 제공해야 한다.

5. 제1항 및 제2항에 규정된 의무는 직원 250인 미만의 기업이나 조직에는 적용되지 않는다. 단, 해당 기업이 수행하는 처리가 정보주체의 권리와 자유에 위험을 초래할 것으로 예상되거나, 간헐적이지 않거나, 제9조(1)에 규정된 특정 범주의 개인정보를 포함하거나, 제10조에 규정된 범죄경력 및 범죄행위에 관련된 개인정보를 다루는 경우는 예외로 한다.

제31조
감독기관과의 협력

컨트롤러와 프로세서, 그리고 해당하는 경우, 컨트롤러나 프로세서의 대리인은 요청 시 직무를 수행함에 있어 감독기관과 협력해야 한다.

제2절
개인정보의 보안

제32조

처리의 보안

1. 컨트롤러와 프로세서는 개인정보의 처리가 자연인의 권리 및 자유에 미치는 위험의 다양한 가능성 및 정도와 함께 최신 기술, 실행 비용, 그리고 처리의 성격, 범위, 상황 및 목적을 고려하여, 해당 위험에 적정한 보안 수준을 보장하기 위해 특히 다음 각 호 등을 포함하여 적정한 기술 및 관리적 조치를 이행해야 한다.

(a) 개인정보의 가명처리 및 암호처리

(b) 처리 시스템 및 서비스의 지속적인 기밀성과 무결성, 가용성, 복원력을 보장할 수 있는 역량

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

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

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

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

4. 컨트롤러와 프로세서는 컨트롤러나 프로세서의 권한에 따라 개인정보를 열람하는 모든 자연인이 유럽연합 또는 회원국 법률로 요구되는 것이 아니라면 컨트롤러의 지시에 따른 경우를 제외하고는 개인정보를 처리하지 못하도록 해야 한다.

제33조

감독기관에 대한 개인정보 침해 통지

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

2. 프로세서는 개인정보의 침해를 알게 된 후 부당한 지체 없이 컨트롤러에게 이를 통지해야 한다.

3. 제1항에서 규정한 통지는 최소한 다음 각 호를 포함해야 한다.

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

(b) 데이터보호담당관, 그리고 더 많은 정보를 얻을 수 있는 경우, 기타 연락 가능한 개인의 이름 및 상세 연락처 전달

(c) 개인정보 침해로 인해 발생할 수 있는 결과에 대한 설명

(d) 적절한 경우, 개인정보 침해로 인한 부작용을 완화하기 위한 조치 등, 해당 개인정보 침해 해결을 위해 컨트롤러가 취하거나 취하도록 제안되는 조치에 대한 설명

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

5. 컨트롤러는 개인정보 침해와 관련된 사실, 유출로 인한 영향, 이에 대해 시행된 시정 조치 등, 모든 개인정보 침해 건을 문서화해야 한다.

제34조

정보주체에 대한 개인정보 침해 통지

1. 개인정보의 침해가 자연인의 권리와 자유에 중대한 위험을 초래할 것으로 예상되는 경우, 컨트롤러는 부당한 지체 없이 정보주체에게 그 개인정보 침해에 대해 통지해야 한다.

2. 본 조 제1항에 규정된 정보주체에 대한 통지에서는 해당 개인정보 유출의 성격을 명확하고 평이한 언어로 기술하고, 최소한 제33조(3)의 (b)호, (c)호, (d)호에 규정된 정보 및 권고를 포함해야 한다.

3. 다음 각 호의 하나에 해당하는 경우, 제1항의 정보주체에 대한 통지는 요구되지 않는다.

(a) 컨트롤러가 적절한 기술적 및 관리적 보호조치를 시행하였고, 그 조치, 특히 암호처리 등 관련 개인정보를 열람 권한이 없는 개인에게 이해될 수 없도록 만드는 조치가 침해로 영향을 받은 개인정보에 적용된 경우

(b) 컨트롤러가 제1항에 규정된 정보주체의 권리와 자유에 대한 중대한 위험을 더 이상

실현될 가능성이 없도록 만드는 후속 조치를 취한 경우

(c) 필요 이상의 노력이 수반될 수 있는 경우. 이 경우, 공개 또는 유사한 조치를 통해 정보주체가 동등하게 효과적인 방식으로 통지받도록 해야 한다.

4. 컨트롤러가 정보주체에게 개인정보 침해에 대해 아직 통지하지 않은 경우, 관련 감독기관은 중대한 위험을 초래하는 개인정보 침해의 가능성을 고려한 후, 컨트롤러에게 통지하도록 요구하거나 제3항의 어느 조건이라도 충족시키도록 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 것으로 예상되는 경우, 컨트롤러는 처리 이전에, 예정된 처리 작업이 개인정보 보호에 미치는 영향에 대한 평가를 수행해야 한다. 한 번의 평가로 유사한 중대한 위험을 초래하는 일련의 유사 처리 작업을 다룰 수 있다.

2. 컨트롤러는 데이터보호담당관이 지정된 경우, 개인정보보호 영향평가를 수행할 때, 담당관의 자문을 구해야 한다.

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

(a) 프로파일링 등의 자동화된 처리에 근거한, 개인에 관한 개인적 측면을 체계적이고 광범위하게 평가하는 것으로 해당 평가에 근거한 결정이 해당 개인에게 법적 효력을 미치거나 이와 유사하게 개인에게 중대한 영향을 미치는 경우

(b) 제9조(1)에 규정된 특별 범주의 개인정보에 대한 대규모 처리나 제10조에 규정된 범죄경력 및 범죄 행위에 관련된 개인정보에 대한 처리

(c) 공개적으로 접근 가능한 지역에 대한 대규모의 체계적 모니터링

4. 감독기관은 제1항에 따라 개인정보보호 영향평가의 요건이 적용되는 처리 작업의 종류의 목록을 작성 및 공개해야 한다. 감독기관은 제68조에 규정된 유럽 데이터보호이사회에 해당 목록을 통보해야 한다.

5. 감독기관은 개인정보보호 영향평가가 요구되지 않는 처리 작업의 종류의 목록 또한

작성하여 공개할 수 있다. 감독기관은 유럽 데이터보호이사회에 해당 목록을 통보해야 한다.

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

7. 평가는 최소한 다음의 각 호를 포함해야 한다.

(a) 예상되는 처리 작업 및 컨트롤러의 정당한 이익 등 개인정보 처리의 목적에 대한 체계적인 설명

(b) 목적과 관련한 처리 작업의 필요성 및 비례성에 대한 평가

(c) 제1항에 규정된 정보주체의 권리와 자유에 대한 위험성 평가;

(d) 정보주체와 기타 관련인의 권리 및 정당한 이익을 고려하여 개인정보의 보호를 보장하고 본 규정의 준수를 입증하기 위한 안전조치, 보안조치, 메커니즘 등 위험성 처리에 예상되는 조치

8. 특히 개인정보보호 영향평가를 위해 관련 컨트롤러나 프로세서가 수행하는 처리 작업의 영향을 평가할 때는 해당 컨트롤러나 프로세서가 제40조의 승인된 행동강령을 준수하는 것을 고려해야 한다.

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

10. 제6조(1)의 (c)호 또는 (e)호에 따른 처리가 컨트롤러에 적용되는 유럽연합 또는 회원국 법률 내에 법적 근거를 두고 있는 경우로서, 해당 법률이 특정 처리 작업이나 일련의 관련 작업을 규제하고 개인정보보호 영향평가가 이미 그 법적 근거를 채택하는 중에 일반적 영향평가의 일환으로 시행된 경우, 제1항에서 제7항까지 적용되지 않는다. 단, 회원국이 처리활동 이전에 이러한 영향평가의 수행이 필요하다고 고려하는 경우는 예외로 한다.

11. 필요하다면, 컨트롤러는 적어도 처리 작업으로 초래되는 위험에 변화가 있을 시에는 처리가 개인정보보호 영향평가에 따라 실시되는지를 평가하기 위한 검토를 시행해야 한다.

제36조

사전 자문

1. 제35조에 따른 개인정보보호 영향평가를 통해 처리가 고위험의 결과를 초래하는 경우로서 컨트롤러가 그 위험을 완화하기 위해 취한 조치가 부재한 것으로 나타나는 경우 해당 처리 전 감독기관의 자문을 구해야 한다.

2. 감독기관이 제1항의 예정된 처리가 본 규정을 위반할 것이라는 의견을 제시하는 경우로서 특히 컨트롤러가 위험을 충분히 파악하거나 완화하지 못한 경우, 감독기관은 자문 요청을 접수한지 8주의 기간 내에 해당 컨트롤러에게 서면 형식의 권고를 제공해야 하고, 해당하는 경우 프로세서에게도 제공해야 하며, 제58조에 규정된 어느 권한이라도 사용할 수가 있다. 해당 기간은 예정된 처리의 복합성을 고려하여 6주까지 연장될 수 있다. 감독기관은 자문 요청을 접수한 후 한 달 내에 컨트롤러에게, 그리고 해당하는 경우 프로세서에게도 지연의 사유와 함께 그 같은 기간 연장에 대해 알려야 한다. 그 기간은 감독기관이 자문의 목적으로 요청한 정보를 입수할 때까지 연기될 수 있다.

3. 제1항에 따라 감독기관의 자문을 구할 때, 컨트롤러는 다음 각 호를 감독기관에 제공해야 한다.

(a) 가능한 경우, 처리에 관여하는 컨트롤러, 공동 컨트롤러 및 프로세서의 개별 책임, 특히 사업체집단 내의 처리에 대한 책임

(b) 예정된 처리의 목적 및 방법

(c) 본 규정에 따라 정보주체의 권리와 자유를 보호하기 위해 제공되는 조치 및 안전조치

(d) 가능한 경우, 데이터보호담당관의 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 구해야 한다.

5. 제1항에 관계없이, 회원국 법률은 사회 보호 및 공중 보건과 관련된 처리 등, 컨트롤러가 공익을 위해 소관업무를 수행함에 있어 정보를 처리하는 것과 관련하여, 컨트롤러가 감독기관에게 자문을 구하고 사전 승인을 획득하도록 요구할 수 있다.

제4절

데이터보호담당관

제37조

데이터보호 담당관의 지정

1. 다음 각 호에 해당하는 경우, 컨트롤러와 프로세서는 데이터보호담당관을 지정해야 한다.

(a) 법원이 사법 권한을 행사하는 경우를 제외한 공공당국 또는 기관이 처리를 하는 경우

(b) 컨트롤러나 프로세서의 핵심 활동이 처리의 성격, 범위 또는 목적에 의해 정보주체에 대한 정기적이고 체계적인 대규모의 모니터링을 요하는 처리 작업들로 구성되는 경우

(c) 컨트롤러 또는 프로세서의 핵심 활동이 제9조에 따른 특별 범주의 개인정보와 제10조에 규정된 범죄경력 및 범죄 행위에 관련된 개인정보를 대규모로 처리하는 것으로 구성되는 경우

2. 사업체 집단은 단일의 데이터보호담당관을 지정할 수 있는데, 각 사업장이 해당 데이터보호담당관을 쉽게 이용할 수 있는 경우에 그러하다.

3. 컨트롤러 또는 프로세서가 공공당국이나 기관인 경우, 조직의 구조나 규모를 고려하여, 다수의 그러한 당국이나 기관을 위해 단일의 데이터보호담당관이 지정될 수 있다.

4. 제1항에 규정된 것 이외의 경우, 컨트롤러나 프로세서의 각 범주를 대표하는 협회 또는 기타 기관은, 유럽연합 또는 회원국 법률이 요구하는 경우, 데이터보호담당관을 지정할 수 있거나 지정해야 한다. 데이터보호담당관은 컨트롤러 또는 프로세서를 대변하는 해당 협회 및 기타 기관을 대행할 수 있다.

5. 데이터보호담당관은 직무상의 자질, 특히 개인정보 보호법과 실무에 대한 전문가적 지식과 제39조에 규정된 업무를 수행할 수 있는 능력에 근거하여 지정되어야 한다.

6. 데이터보호담당관은 컨트롤러 또는 프로세서의 직원일 수 있거나, 서비스계약에 근거하여 업무를 수행할 수 있다.

7. 컨트롤러 또는 프로세서는 데이터보호담당관의 상세 연락처를 공개하며 이를 감독기관에 통보하여야 한다.

제38조
데이터보호담당관의 지위

1. 컨트롤러 및 프로세서는 데이터보호담당관이 개인정보 보호와 관련된 모든 문제에 적절하고 시의 적절하게 관여하도록 해야 한다.

2. 컨트롤러 및 프로세서는 데이터보호담당관이 제39조의 업무를 수행하고 개인정보 및

처리 작업을 열람하며 전문지식을 유지하는 데 필요한 자원을 제공함으로써 그의 업무 수행을 지원해야 한다.

3. 컨트롤러 또는 프로세서는 데이터보호담당관이 그 업무의 수행에 있어 어떠한 지시도 받지 않도록 보장해야 한다. 데이터보호담당관은 본인의 업무 수행을 이유로 컨트롤러나 프로세서에 의해 해임 또는 처벌받아서는 안 된다. 데이터보호담당관은 컨트롤러 또는 프로세서의 최고 경영진에게 직접 보고해야 한다.

4. 정보주체는 본인의 개인정보 처리 및 본 규정에 따른 권리 행사와 관련한 모든 사안에 관해 데이터보호담당관에 연락을 취할 수 있다.

5. 데이터보호담당관은 유럽연합이나 회원국 법률에 따라 본인의 업무 수행에 관해 비밀 또는 기밀유지의 의무를 준수해야 한다.

6. 데이터보호담당관은 기타 업무 및 직무를 수행할 수 있다. 컨트롤러나 프로세서는 이러한 업무 및 직무가 이해의 상충을 초래하지 않도록 해야 한다.

제39조

데이터보호담당관의 업무

1. 데이터보호담당관은 최소한 다음 각 호의 업무를 수행하여야 한다.

(a) 컨트롤러 또는 프로세서, 그리고 처리를 수행하는 직원에게 본 규정과 유럽연합 또는 회원국의 개인정보 보호 규정에 따른 의무에 대해 고지 및 권고

(b) 책임 할당, 인식 제고, 처리 작업에 관련된 직원 교육 및 관련 감사 등 본 규정, 기타 유럽연합 또는 회원국의 개인정보 보호 규정, 개인정보 보호와 관련한 컨트롤러 또는 프로세서의 정책이 준수되는지 모니터링

(c) 요청이 있을 경우, 제35조에 따라 개인정보보호 영향평가에 관한 자문 제공 및 평가의 이행을 모니터링

(d) 감독기관과 협력

(e) 제36조에 규정된 사전 자문 등, 처리에 관련한 현안에 대해 감독기관의 연락처의 역할 수행 및 적절한 경우, 기타 사안에 대한 자문 제공

2. 데이터보호담당관은 업무를 수행할 때 처리의 성격과 범위, 상황, 목적을 참작하여 처리 작업과 연계된 위험을 충분히 고려해야 한다.

제5절
행동강령 및 인증

제40조
행동강령

1. 회원국, 감독기관, 유럽 데이터보호이사회, 집행위원회는 다양한 처리 부문의 명확한 특징과 영세 및 중소기업의 특정 요구를 고려하여 본 규정을 적절히 적용하기 위한 취지의 행동강령을 입안하도록 장려한다.

2. 컨트롤러나 프로세서의 각 범주를 대표하는 협회(associations) 또는 기타 기관은 다음 각 호와 관련하여 본 규정의 적용을 구체화할 목적으로 행동강령을 제정하거나 해당 강령을 수정 또는 확대할 수 있다.

(a) 공정하고 투명한 처리

(b) 특정 상황에서의 컨트롤러의 정당한 이익

(c) 개인정보의 수집

(d) 개인정보의 가명처리

(e) 일반 및 정보주체에게 제공되는 정보

(f) 정보주체의 권리 행사

(g) 아동에게 제공되는 정보 및 아동의 보호, 아동에 대한 친권을 보유한 자의 동의를 획득하는 방식

(h) 제24조 및 제25조에 규정된 조치 및 절차, 제32조에 규정된 처리의 안전을 보장하기 위한 조치

(i) 감독기관 및 정보주체에게 개인정보 침해에 대해 통지

(j) 제3국이나 국제기구로 개인정보 이전

(k) 제77조 및 제79조에 따른 정보주체의 권리를 침해하지 않고, 처리와 관련하여 컨트롤러와 정보주체 간의 분쟁을 해결하기 위한 재판 외 절차 및 기타 분쟁해결 절차

3. 본 규정을 적용 받는 컨트롤러 또는 프로세서의 규정 준수와 더불어, 제3조에 따라 본 규정을 적용 받지 않는 컨트롤러 또는 프로세서는 제46조(2) (e)호의 조건에 따라 제3국 또는 국제기구로의 개인정보 이전에 대한 프레임워크 안에서 적정한 안전조치를 제공하기 위해 본 조 제5항에 따라 승인된 행동강령과 본 조 제9항에 따라 일반적인 효력을 가지는 행동강령을 준수할 수 있다. 해당 컨트롤러 또는 프로세서는 계약 증서 또는 기타의 법적 구속력이 있는 장치를 통해, 정보주체의 권리에 관해서 등 상기의 적정한 안전조치를 적용하기 위해 구속력 있고 강제할 수 있는 약속을 해야 한다.

4. 본 조 제2항의 행동강령은 제41조(1)에 규정된 기관이 제55조와 제56조에 따른 감독기관의 업무와 권한을 침해하지 않고, 행동강령을 적용하기로 약속한 컨트롤러와 프로세서가 해당 조문을 준수하는 것을 의무적으로 모니터링 할 수 있도록 하는 메커니즘을 포함해야 한다.

5. 행동강령을 작성하거나 기존 강령을 개정 또는 확대할 의도인 본 조 제2항의 협회 또는 기타 기관은 제55조에 따른 권한을 가지는 감독기관에 강령 초안이나 개정 또는 확대 강령을 제출해야 한다. 감독기관은 강령 초안이나 개정 또는 확대 강령이 본 규정에 부합하는지 여부에 대한 의견을 제시하고 적정한 안전조치를 제공한다고 판단되는 경우, 해당 초안이나 개정 또는 확대 강령을 승인해야 한다.

6. 강령 초안이나 개정 또는 확대 강령이 제5항에 따라 승인되는 경우, 또한 해당 행동강령이 복수 회원국에서의 처리 활동과 관련되지 않을 경우, 감독기관은 그 강령을 등록 및 공개해야 한다.

7. 행동강령 초안이 복수 회원국에서의 처리 활동에 관련될 경우, 제55조에 따른 권한을 가지는 감독기관은 강령 초안이나 개정 또는 확대 강령을 승인하기 전에 제63조에 규정된 절차에 따라 유럽 데이터보호이사회에 이를 제출해야 하며, 이사회는 강령 초안이나 개정 또는 확대 강령이 본 규정을 준수하는지 여부, 또는 제3항에 규정된 상황에서, 적정한 안전조치를 제공하는지 여부에 대한 의견을 제시해야 한다.

8. 제7항에 명시된 의견이 해당 강령 초안이나 개정 또는 확대 강령이 본 규정을 준수한다고 확정하거나 제3항에 규정된 상황에서 적정한 안전조치를 제공한다고 확정하는 경우, 유럽 데이터보호이사회는 본 의견을 집행위원회에 제출해야 한다.

9. 집행위원회는 이행 법률을 통해 제8항에 따라 제출된 승인된 행동강령이나 개정 또는 확대 강령이 유럽연합 내 일반적인 효력을 가진다고 결정할 수 있다. 그 이행 법률은 제93조(2)에 규정된 심사 절차에 따라 채택되어야 한다.

10. 집행위원회는 제9항에 따라 일반적 효력을 가진다고 결정이 내려진 승인된 강령이 적절히 홍보되도록 해야 한다.

11. 유럽 데이터보호이사회는 승인된 행동강령과 개정 또는 확대된 강령 일체를 등록부에 취합하고 적절한 수단을 통해 이를 공개해야 한다.

제41조

승인된 행동강령의 모니터링

1. 제57조와 제58조에 따른 관련 감독기관의 업무와 권한을 침해하지 않으면서, 제40조에 따른 행동강령의 준수에 대한 모니터링은 행동강령의 주제와 관련하여 적정 수준의 전문지식을 보유하고, 관련 감독기관이 그 목적으로 승인한 기관이 실시할 수 있다.

2. 제1항의 기관은 다음 각 호에 해당하는 경우 행동강령의 준수를 모니터링 하도록 승인받을 수 있다.

(a) 감독기관이 만족할 수준의 독립성 및 강령의 주제와 관련한 전문지식을 입증한 경우

(b) 강령을 적용하는 컨트롤러 및 프로세서의 적격성을 평가하고 관련 조문의 준수를 모니터링하며 강령의 이행을 정기적으로 검토할 수 있도록 하는 절차를 수립한 경우

(c) 강령 위반 및 컨트롤러나 프로세서가 강령을 이행하였거나 이행하는 방식에 관한 민원을 처리하는 절차 및 구조를 수립하고, 그 절차와 구조를 정보주체와 일반에 투명하게 할 절차 및 구조를 수립한 경우

(d) 그 업무와 직무가 이해의 상충을 초래하지 않는다는 사실을 관련 감독기관이 만족할 정도로 입증하는 경우.

3. 관련 감독기관은 제63조의 일관성 메커니즘에 따라, 본 조 1항에 규정된 기관을 인증하기 위한 기준의 초안을 유럽 데이터보호이사회에 제출해야 한다.

4. 관련 감독기관의 업무와 권한 및 제VIII장의 조문을 침해하지 않고, 제1항에 규정된 기관은 컨트롤러 또는 프로세서가 강령을 위반하는 경우 적정한 안전조치에 따라 강령 이행의 중지나 배제 등의 적절한 조치를 취해야 한다. 해당 기관은 해당 조치와 해당 조치 사유를 감독기관에 통지해야 한다.

5. 인증 조건이 충족되지 않거나 더 이상 충족되지 않는 경우 또는 제1항의 기관이 취한 조취가 본 규정을 위반하는 경우 관련 감독기관은 그 기관의 인증을 철회해야 한다.

6. 본 조문은 공공기관 및 기타 기관이 시행하는 처리에는 적용되지 않는다.

제42조

인증

1. 회원국과 감독기관, 유럽 데이터보호이사회, 집행위원회는 컨트롤러가 시행하는 처리 작업이 본 규정을 준수하고 있음을 입증하기 위한 목적으로 특히 유럽연합의 차원의 개인정보보호 인증 메커니즘, 개인정보보호 인장 및 마크의 수립을 장려해야 한다. 영세기업이나 중소기업의 특정 요구도 참작되어야 한다.

2. 본 규정을 적용받는 컨트롤러 또는 프로세서의 규정 준수와 더불어, 제46조(2) (f)호의 조건에 따른 제3국 또는 국제기구로의 개인정보 이전이라는 프레임워크 내에서 제3조에 의거 본 규정을 적용받지 않는 컨트롤러 또는 프로세서가 제공하는 적정한 안전조치의 존재를 입증할 목적으로 본 조 제5항에 따라 승인된 개인정보 보호 인증 메커니즘, 인장 또는 마크가 수립될 수 있다. 해당 컨트롤러나 프로세서는 정보주체의 권리와 관련해서 등, 상기의 적정한 안전조치를 적용하기 위해 계약적 또는 기타 구속력 있는 장치를 통해 구속력 및 강제력 있는 약속을 해야 한다.

3. 인증은 자발적이어야 하고 투명한 절차를 통해 제공되어야 한다.

4. 본 조문에 따른 인증이 본 규정을 준수해야 하는 컨트롤러 또는 프로세서의 책임을 경감하지는 않으며, 제55조 또는 제56조에 따라 권한을 가지는 감독기관의 업무와 권한을 침해하지 않는다.

5. 본 조문에 따른 인증은 제58조(3)항에 따른 관련 감독기관이나 제63조에 따른 유럽 데이터보호이사회가 승인한 기준을 토대로, 제43조의 인증기관 또는 관련 감독기관이 발급할 수 있다. 해당 기준이 유럽 데이터보호이사회에 의해 승인되는 경우, 이는 공동 인증인 유럽 데이터보호 인장(European Data Protection Seal)으로 이어질 수 있다.

6. 인증 메커니즘에 처리(정보)를 제출하는 컨트롤러나 프로세서는 제43조의 인증기관이나 해당하는 경우 관련 감독기관에 인증절차를 실시하는 데 필요한 정보 및 처리활동에 대한 접근 일체를 제공해야 한다.

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

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

제43조

인증기관

1. 제57조 및 제58조에 따라 권한을 가지는 감독기관의 업무와 권한을 침해하지 않고

개인정보 보호와 관련하여 적정 수준의 전문지식을 보유한 인증기관은 필요한 경우 감독기관이 제58조(2) (h)호에 따른 권한을 행사할 수 있도록 감독기관에 통지한 후 인증을 발급 및 갱신하여야 한다. 회원국은 그러한 인증기관이 다음 각 호의 하나 또는 모두에 의해 인증 받았음을 보장해야 한다.

(a) 제55조나 제56조에 따라 권한을 가지는 감독기관

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

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

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

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

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

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

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

3. 제1항 및 제2항의 인증기관의 인증은 제55조 또는 제56조에 따라 권한을 가지는 감독기관 또는 제63조에 따라 유럽 데이터보호이사회가 승인한 기준을 근거로 이루어져야 한다. 본 조 제1항 (b)호에 따른 인증의 경우, 본 요건은 규정(EC) 765/2008에서 예상되는 요건과 해당 인증기관의 방법과 절차를 기술하는 기술 규칙을 보완해야 한다.

4. 제1항의 인증기관은 컨트롤러나 프로세서가 본 규정을 준수해야 할 책임을 침해하지 않고 인증 또는 그러한 인증의 철회를 초래하는 적절한 평가에 대한 책임을 져야 한다. 인증은 최대 5년의 기간 동안 발급되며 해당 인증기관이 본 조에 규정된 요건을 충족하는 경우에 한해 동일한 조건으로 갱신될 수 있다.

5. 제1항에 규정된 인증기관은 감독기관에 요청된 인증의 승인 또는 철회의 사유를 제공해야 한다.

6. 감독기관은 쉽게 이용할 수 있는 양식으로 본 조 제3항의 요건과 제42조(5)항의 기준을 공개해야 한다. 아울러 감독기관은 유럽 데이터보호이사회에 해당 요건과 기준을 전송해야 한다. 유럽 데이터보호이사회는 인증 메커니즘과 개인정보 보호 인장 일체를 등록부에 취합하고 적절한 수단을 통해 이를 공개해야 한다.

7. 인증 조건이 충족되지 않거나 더 이상 충족되지 않는 경우, 또는 인증기관이 취한 조치가 본 규정을 위반하는 경우, 관련 감독기관이나 국가 인증기관은 제VIII장의 규정을 침해하지 않고 제1항의 인증기관의 인증을 철회해야 한다.

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

9. 집행위원회는 인증 메커니즘과 개인정보 보호 인장과 마크에 대한 기술적 기준과 이러한 인증 메커니즘을 홍보하고 인정하는 메커니즘을 규정하는 이행 법률을 채택할 수 있다. 해당 이행 법률은 제93조(2)에 규정된 심사 절차에 따라 채택되어야 한다.

제V장
제3국 및 국제기구로의 개인정보 이전

제44조
이전을 위한 통칙

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

제45조
적정성 결정에 따른 이전

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

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

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

(b) 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

(c) 특히 개인정보 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 조 2항의 의미 내에서 적정한 보호 수준을 보장하는지를 판단할 수 있다. 이행 법률은 최소한 4년마다의 정기적 검토를 위한 메커니즘을 규정해야 하고 검토에는 제3국이나 국제기구 내의 관련 추이사항 일체가 고려되어야 한다. 이행 법률은 영토 및 부문별 적용에 대한 규정을 명시하고, 적용이 가능한 경우 본 조 제2항 (b)호의 감독기관(들)에 대해 확인해야 한다. 이행 법률은 제93조(2)의 검토 절차에 따라 채택되어야 한다.

4. 집행위원회는 본 조 제3항에 준하여 채택된 결정 및 지침 95/46/EC의 제25조(6)항을 근거로 채택된 결정의 작동에 영향을 미칠 수 있는 제3국 및 국제기구 내의 추이사항을 지속적으로 모니터링 해야 한다.

5. 집행위원회는 가용 정보를 통해, 특히 제3항에 명시된 검토 이후 제3국, 해당 제3국의 영토나 하나 이상의 지정 부문, 또는 국제기구가 제2항에서 의미하는 적정한 보호 수준을 더 이상 보장하지 않는다고 판단될 경우, 필요한 정도까지 소급효 없이 제3항의 결정을 철회, 수정, 또는 중지시킬 수 있다. 이행 법률은 제93조(2)의 검토 절차를 따라 채택되어야 한다.

충분히 타당하고 긴요한 시급성의 근거가 있는 경우, 제93조(3)의 절차에 따라 집행위원회는 즉시 적용 가능한 이행 법률을 채택하여야 한다.

6. 집행위원회는 제5항에 의거하여 내린 결정을 초래한 상황을 시정할 목적으로 제3국이나 국제기구와 협의해야 한다.

7. 제5항에 의거한 결정은 제46조부터 제49조까지에 따른 해당의 제3국, 제3국의 영토나 하나 이상의 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/EC의 제25조(6)를 근거로 집행위원회가 채택하는 결정은 본 조 제3항 또는 제5항에 따라 채택되는 집행위원회 결정으로 수정, 대체, 폐지될 때까지 유효해야 한다.

제46조

적정한 안전조치에 의한 이전

1. 제45조(3)에 의거한 결정이 없을 경우, 컨트롤러나 프로세서는 적정한 안전조치를 제공한 경우에 한하여, 정보주체가 행사할 수 있는 권리와 유효한 법적 구제책이 제공되는 조건으로 제3국 또는 국제기구에 개인정보를 이전할 수 있다.

2. 제1항의 적정한 안전조치는 감독기관의 특별한 승인을 요하지 아니하고 다음 각 호에 의해 제공될 수 있다.

(a) 공공당국 또는 기관 간에 법적 구속력이 있고 강제할 수 있는 장치

(b) 제47조에 따른 의무적 기업 규칙

(c) 제93조(2)의 검토 절차에 따라 집행위원회가 채택한 정보보호 표준조항

(d) 감독기관이 채택하고 제93(2)조의 검토 절차에 따라 집행위원회가 승인한 정보보호 표준조항

(e) 정보주체의 권리에 관한 것 등 적정한 안전조치를 적용하기 위한 것으로 법적 구속력 및 강제력이 있는 제3국의 컨트롤러나 프로세서의 약속을 포함한 제40조에 의거한 공인 행동강령

(f) 정보주체의 권리에 관한 것 등 적정한 안전조치를 적용하기 위한 것으로 법적 구속력 및 강제력이 있는 제3국의 컨트롤러나 프로세서의 약속을 포함한 제42조에 의거한 공인 인증 메커니즘

3. 제1항의 적정한 안전조치는 관할 감독기관의 승인을 거쳐 특히 다음 각 호를 통해서도 제공될 수 있다.

(a) 컨트롤러나 프로세서와 제3국이나 국제기구의 컨트롤러, 프로세서 또는 개인정보 수령인 간의 계약 조항

(b) 공공당국이나 기관 간의 행정 협정에 삽입될 것으로 강제력이 있고 유효한 정보주체의 권리를 포함한 규정

4. 감독기관은 본 조 제3항의 사례의 경우 제63조의 일관성 메커니즘을 적용해야 한다.

5. 지침 95/46/EC의 제26조(2)를 근거로 한 회원국이나 감독기관의 승인은 필요한 경우 해당 감독기관이 수정, 대체, 철회할 때까지 유효해야 한다. 지침 95/46/EC의 제26조(4)를 근거로 집행위원회가 채택하는 결정은 필요한 경우 본 조 제2항에 따라 채택된 집행위원회 결정에 의해 수정, 대체 또는 철회될 때까지 유효해야 한다.

제47조

의무적 기업 규칙

1. 관할 감독기관은 제63조에 명시된 일관성 메커니즘에 따라 의무적 기업 규칙을 승인해야 한다. 단, 그 규칙이 다음 각 호를 전제로 해야 한다.

(a) 법적 구속력이 있으며 피고용인 등 공동 경제활동에 관여하는 사업체 집단 또는 기업 집단의 모든 구성원들에게 적용되고 그들에 의해 이행되는 경우

(b) 본인의 개인정보 처리와 관련하여 정보주체에게 명시적으로 구속력 있는 권리를 부여하는 경우

(c) 제2항의 요건을 충족시키는 경우

2. 제1항의 의무적 기업 규칙은 최소한 다음 각 호를 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 확인 등의 정보 이전 또는 이전 건 일체

(c) 내외부적으로 법적 구속력이 있는 특성

(d) 특히 목적제한과 데이터 최소화, 보관기간 제한, 정보 품질, 설계 및 기본설정에 의한 정보보호, 정보처리의 법적 근거, 특별 범주의 개인정보 처리, 정보 보안 확보 대책 등의

일반 정보보호 원칙 및 향후 의무적 기업 규칙의 구속을 받지 않는 기관에 대한 재이전과 관련된 요건의 적용

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

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

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

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

(i) 민원 절차

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

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

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

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

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

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

제48조

유럽연합 법률로 승인되지 않은 정보의 이전 또는 제공

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

제49조

특정 상항에 대한 적용의 일부 제외

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

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

(b) 정보주체와 프로세서 간의 계약을 이행하기 위해서나 정보주체의 요청으로 취한 계약 사전 조치를 이행하는 데 이전이 필요한 경우

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

(d) 중요한 공익상의 이유로 정보이전이 필요한 경우

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

(f) 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 일반 국민 또는 정당한 이익을 입증할 수 있는 제3자가 참조(조회)하기 위한 목적으로 만들어진

개인정보 기록부(register)로부터 유럽연합 또는 회원국 법률에 명시된 참조(조회)의 조건이 충족되는 범위 내에서 이전되는 경우

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

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

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

4. 제1항 (d)호의 공익은 컨트롤러가 적용받는 유럽연합 또는 회원국 법률에서 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. 컨트롤러나 프로세서는 제30조의 기록부(records)에 본 조 제1항의 두 번째 단락에 명시된 평가 및 적절한 안전조치를 기록해야 한다.

제50조

개인정보 보호를 위한 국제협력

집행위원회와 감독기관은 제3국 및 국제기구와 관련하여 다음 각 호를 위한 적절한 조치를 시행해야 한다.

(a) 개인정보 보호를 위한 법률의 효과적인 집행을 위한 국제협력 메커니즘 개발

(b) 개인정보 및 기타 기본적 권리와 자유를 보호하기 위한 적정한 안전조치에 따라, 통지,

민원 이첩, 조사 지원 및 정보 교환을 통해서 등 개인정보 보호를 위한 법률 집행에 대한 국제 상호 지원 제공

(c) 개인정보 보호를 위한 법률 집행 과정에서 국제협력을 촉진시킬 목적으로 논의 및 활동에 이해 당사자들을 참여시킬 것

(d) 제3국과의 사법권 분쟁에 관한 것 등 개인정보 보호 법률 및 관행에 대한 교류 및 문서화를 촉진

제VI장
독립적인 감독기관

제1절
독립적인 지위

제51조
감독기관

1. 각 회원국은 처리와 관련하여 개인의 기본권과 자유를 보호하고 유럽연합 역내에서 개인정보의 자유로운 이전을 촉진하기 위하여, 본 규정의 적용에 대한 모니터링을 전담할 하나 이상의 독립적인 공공기관을 제공해야 한다.

2. 각 감독기관은 유럽연합 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 유럽 데이터보호이사회에서 해당 감독기관들을 대표할 감독기관을 지정하고 제63조에 규정된 일관성 메커니즘과 관련한 규정을 다른 기관이 준수하도록 보장하는 메커니즘을 수립해야 한다.

4. 각 회원국은 제VI장에 의거하여 채택한 자국 법률의 조항을 2018년 5월 25일까지 지체 없이 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 유럽 데이터보호이사회에의 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 다음의 투명한 절차를 통해 임명되도록 해야 한다.

- 의회
- 정부
- 국가 수장
- 회원국 법률에 의해 임명이 위임된 독립적 기관

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 설립에 관한 규칙

각 회원국은 다음을 법률로 규정한다.

(a) 각 감독기관의 설립

(b) 각 감독기관의 위원으로 임명되는데 필요한 자격과 적격 조건

(c) 각 감독기관 위원(들)의 임명 규칙 및 절차

(d) 본 규제의 발효 후 첫 임명을 제외하고, 4년 이상의 각 감독기관의 위원(들)의 임기. 단, 시차를 둔 임명 절차를 활용하여 감독기관의 독립성을 보호하기 위해 필요할 경우, 임기 중 일부를 단축할 수 있다

(e) 각 감독기관 위원(들)의 재임명 가능여부 및 임기 연장의 횟수

(f) 각 감독기관의 임직원의 의무에 관한 조건, 임기 도중과 이후 그에 양립되지 않는 행위나 직업, 편익에 대한 금지, 고용 중단에 관한 규칙

2. 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)의 (c) 또는 (e)호를 근거로 활동하는 공공기관이나 민간기관에 의해 처리가 수행되는 경우, 해당 회원국의 감독기관은 이에 대한 법적자격을 갖는다. 이 경우 제56조는

적용되지 아니한다.

3. 감독기관은 사법능력을 행사하는 법원의 처리방식을 감독할 법적 자격은 없다.

제56조

선임 감독기관의 법적 자격

1. 컨트롤러 또는 프로세서의 주 사업장이나 단일 사업장의 감독기구는, 제55조를 침해하지 않으면서, 제60조에 규정된 절차에 따라 컨트롤러 또는 프로세서가 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 조 제2항에 규정된 상황의 경우, 해당 감독기관은 지체 없이 관련 사안에 대해 선임 감독기관에 통지해야 한다. 통지를 받은 후 3주 이내에, 선임 감독기관은 감독기관이 고지한 회원국의 컨트롤러 또는 프로세서의 사업장의 존재 여부를 고려하여, 제60조에 규정된 절차에 따라, 해당 상황을 처리할 지 여부를 결정해야 한다.

4. 선임 감독기관이 관련 상황을 처리하기로 결정할 경우, 제60조에 규정된 절차가 적용된다. 선임 감독기관에 통보한 감독기관은 선임 감독기관에 결정문의 초안을 제출한다. 선임 감독기관은 제60조(3)에 규정된 결정문 초안을 작성할 때, 해당 초안을 최대한 고려해야 한다.

5. 선임 감독기관이 관련 상황을 처리하지 않기로 결정할 경우, 선임 감독기관에 통보한 감독 기관은 제61조와 제62조에 의거하여 해당 상황을 처리해야 한다.

6. 선임 감독기관은 컨트롤러나 프로세서가 수행하는 회원국 간의 처리에 대해 컨트롤러 또는 프로세서의 유일한 교섭담당기관이다.

제57조

업무

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

(a) 본 규정의 적용에 대한 모니터링 및 집행

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

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

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

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

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

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

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

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

(l) 제36조(2)에 규정된 처리 작업에 관한 자문 제공

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

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

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

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

(q) 제41조에 의거한 행동강령의 모니터링 기관 및 제43조에 의거한 인증기관의 인증 시행

(r) 제46조(3)에 규정된 계약조항 및 조문에 대한 승인

(s) 제47조에 의거한 의무적 기업규칙에 대한 승인

(t) 유럽 데이터보호이사회의 활동에 기여

(u) 본 규정의 위반과 제58조(2)에 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 제1항 (f)호에 규정된 민원의 제출을 용이하게 한다.

3. 각 감독기관의 업무 수행에 대한 비용은 정보주체의 경우 무료이며, 해당되는 경우, 데이터보호담당관도 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 감독기관은 아래의 조사 권한을 모두 보유한다.

(a) 컨트롤러와 프로세서 그리고 해당되는 경우, 컨트롤러 또는 프로세서의 대리인에게 업무의 수행에 필요한 정보의 일체를 제공하도록 명령

(b) 개인정보보호 감사의 형식의 조사 실시

(c) 제42조(7)에 의거하여 발급된 인증에 대한 검토 실시

(d) 컨트롤러 또는 프로세서에게 본 규정의 위반 혐의 사안의 통지

(e) 컨트롤러 또는 프로세서로부터 업무 수행에 필요한 모든 개인정보 및 모든 정보에 대한 열람권 취득

(f) 유럽연합 또는 회원국의 절차 법률에 따라, 모든 개인정보 처리 장치 및 수단 등, 컨트롤러와 프로세서의 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 컨트롤러 또는 프로세서에게 경고 발령

(b) 예정된 처리작업(들)이 본 규정의 조문을 위반한 경우, 컨트롤러 및 프로세서를 견책

(c) 컨트롤러 및 프로세서가 본 규정에 따라 본인의 권리를 행사하고자 하는 정보주체의 요청을 따를 것을 지시

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

(e) 정보주체에게 개인정보 침해에 대해 통지하도록 프로세서에게 지시

(f) 처리에 대한 금지 등, 임시 또는 확정적 제한 부과

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

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

(i) 각 개별 상황별 정황에 따라 본 조항에 규정된 조치를 부과하거나, 이와 함께 또는 이것 대신, 제83조에 따른 행정적 벌금을 부과

(j) 제3국 또는 국제기구의 수령인으로의 정보 이동의 중지를 지시

3. 각 감독기관은 다음의 모든 승인 및 자문권한을 보유한다.

(a) 제36조에 규정된 사전 자문의 절차에 따라 프로세서에게 자문을 제공

(b) 자체 재량이나 요구에 따라, 해당 국가의 국회, 회원국의 정부 또는 회원국 법률에 따라 기타 기구 및 기관과 일반에 개인정보 보호와 관련한 사안에 대한 의견을 제공

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

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

(e) 제42조에 따른 인증기관의 인증

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

(g) 제28조(8) 및 제46조(2)에 규정된 정보보호 표준조항의 채택

(h) 제46조(3)의 (a)호에 규정된 정보보호 계약조항에 대한 승인

(i) 제46조(3)의 (b)호에 규정된 행정적 협약에 대한 승인

(j) 제47조에 따른 의무적 기업규칙에 대한 승인

4. 본 조문에 따라 감독기관에게 수여된 권한의 행사는 헌장에 따른 유럽연합 및 회원국 법률에 규정된 유효한 사법구제 및 정밀 실사 등, 적절한 안전조치를 적용 받는다.

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)에 따라 취해진 조치의 유형의 목록을 포함할 수 있는 관련 활동에 대한 연차보고서를 작성해야 한다. 해당 보고서는 해당 국가의 의회, 정부, 그리고 회원국 법률이 지정한 관련 기관에 전달되어야 한다. 해당 보고서는 대중, 집행위원회 및 유럽 데이터보호이사회에 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 컨트롤러 또는 프로세서에 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 조 제3항에 따라 자문을 받은 후 4주의 기간 내에 결정(안)에 대하여 적정하고 타당한 반대 의사를 표명할 경우, 선임 감독기관은 이와 같은 적정하고 타당한 반대 의견에 따르지 않거나 그것이 적정하고 타당하지 않다는 의견이 있을 경우, 제63조에서 규정된 일관성 메커니즘에 그 사안을 상정해야 한다.

5. 선임 감독기관이 해당의 적정하고 타당한 반대 의사를 따르고자 할 경우, 의견 수렴을 위해 수정한 결정(안)을 나머지 관련 감독기관에 제출해야 한다. 수정된 결정(안)은 2주의 기간 내에 제4항에 명시된 절차의 적용을 받는다.

6. 어느 관련 감독기관도 제4항 및 제5항에 명시된 기간 내에 선임 감독기관이 제출한 결정(안)에 반대 의사를 표명하지 않은 경우, 선임 감독기관 및 관련 감독기관은 해당 결정(안)에 합의한 것으로 간주되고 그것을 따라야 한다.

7. 선임 감독기관은 해당 결정을 채택하고 컨트롤러 또는 프로세서의 주 사업장이나 단일 사업장에 고지해야 하며, 경우에 따라 나머지 관련 감독기관 및 유럽 데이터보호이사회에도 관련 사실과 근거의 개요 등 해당 결정을 통보해야 한다. 민원을 접수한 감독기관은 민원인에게 결정에 대해 통보해야 한다.

8. 제7항 적용의 일부 제외로 인해 민원이 묵살 또는 거부되는 경우, 해당 민원을 접수한 감독기관은 결정을 채택하고 그 사실을 민원인과 해당 컨트롤러에게 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 컨트롤러와 관련한 조치에 관한 부분에 대해

결정을 채택하고, 자국 영토에 있는 컨트롤러 또는 프로세서의 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 컨트롤러 또는 프로세서에 통보해야 한다.

10. 제7항 및 제9항에 따라 선임 감독기관의 결정을 고지 받은 후, 컨트롤러 또는 프로세서는 유럽연합 내 모든 사업장의 활동 중에 시행되는 데이터 처리에 대하여 그 결정을 준수하기 위해 필요한 조치를 취해야 한다. 컨트롤러 또는 프로세서는 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 제4힝에 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 안 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 제5항에 언급된 정보를 제공하지 않을 경우, 요청 감독기관은 제55(1)조에 의거하여 자국의 영토에서 잠정적 조치를 채택할 수 있다. 이 경우, 제66조(1)의 조치의 시급한 필요성이 충족된 것으로 간주되어야 하고 이로써 제66조(2)에 따라 유럽 데이터보호이사회로부터 구속력 있는 긴급한 결정이 요구된다.

9. 집행위원회는, 이행 법률을 통해, 본 조문에 명시된 상호 지원을 위한 형식과 절차 및 제6항에 명시된 표준 양식 등 감독기관들 간, 그리고 감독기관과 유럽 데이터보호이사회 간에 전자적 수단에 의한 정보 교환 방식을 규정할 수 있다. 이 같은 이행 법률은 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. 컨트롤러 또는 프로세서가 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 공동 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. 제1항에 의거하여, 부속 감독기관의 직원이 타 회원국에서 활동할 경우, 주최 감독기관의 회원국은 해당 기관이 운영되는 회원국의 법률에 따라 업무 중에 발생하는 피해에 대한 책임 등 기관의 활동에 대한 책임을 져야 한다.

5. 피해가 발생한 회원국은 자국 직원이 초래한 피해에 적용되는 조건에 따라 피해를 보상해야 한다. 타 회원국의 영토에서 타인에게 피해를 유발한 직원이 소속된 부속 감독기관의 회원국은 상대 회원국이 피해를 입은 당사자에게 대신 지불한 피해액을 전액 변상해야 한다.

6. 제3자에 대한 권리 행사를 침해하지 않고 제5항을 예외로 하여, 각 회원국은 제1항에 규정된 사례의 경우 제4항에 명시된 피해와 관련하여 타 회원국으로부터의 배상 요구를 자제해야 한다.

7. 공동 작업이 예정되어 있고 감독기관이 한 달 내에 제2항의 두 번째 문장에 규정된 의무를 준수하지 않는 경우, 나머지 감독기관들은 제55조에 따라 자국의 영토에서 잠정적 조치를 채택할 수 있다. 그 같은 경우, 제66조(1)에 규정된 조치의 시급한 필요성이 충족된다고 간주되어야 하고 이로써 제66조(2)에 따라 유럽 데이터보호이사회로부터 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 메커니즘을 통해 상호 간에, 그리고 적정한 경우 집행위원회와 협력해야 한다.

제64조

유럽 데이터보호이사회 의견

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

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

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

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

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

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

(f) 제47조에 규정된 의무적 기업 규칙을 승인하고자 할 경우

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

3. 제1항 및 제2항에 명시된 사례의 경우, 유럽 데이터보호이사회는 동일 사안에 대해 이미 의견서를 발부하지 않았다면 제출 받은 사안에 대해 의견서를 발부해야 한다. 그 의견서는 8주 내에 유럽 데이터보호이사회의 단순 과반수로 채택되어야 한다. 본 기간은 사안의 복잡성을 참작하여 6주간 추가 연장될 수 있다. 제1항에 명시되고 제5항에 따라 이사회 소속 위원에게 회람되는 결정(안)에 대해 의장이 적시한 적정 기간 내에 반대하지 않는 위원은 결정(안)에 동의한 것으로 간주한다.

4. 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 유럽 데이터보호이사회에 부당한 지체 없이 전달해야 한다.

5. 유럽 데이터보호이사회 의장은 부당한 지체 없이 다음의 내용을 통지해야 한다.

(a) 유럽 데이터보호이사회 위원 및 집행위원회에 표준화된 양식을 사용하여 전달된 관련 정보 일체. 유럽 데이터보호이사회 사무국은 필요한 경우 관련 정보의 번역본을 제공해야 한다.

(b) 제1항 및 제2항에 명시된 해당 감독기관과 집행위원회에 의견서 통지 및 일반 공개

6. 제3항에 명시된 기간 내에 관할 감독기관은 제1항에 명시된 결정(안)을 채택해서는 아니 된다.

7. 제1항에 명시된 감독기관은 의견서 접수 후 2주 내에 유럽 데이터보호이사회의 의견을 신중하게 고려한 후 유럽 데이터보호이사회 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 제7항에 명시된 기간 내에 유럽 데이터보호이사회 의장에게 이사회 의견의 전부 또는 일부를 따르지 않겠다는 의사를 적정한 근거와 함께 통보하는 경우, 제65조(1)이 적용되어야 한다.

제65조

유럽 데이터보호이사회의 분쟁 해결

1. 개별 사례에서 본 규정을 정확하고 일관되게 적용하기 위해, 유럽 데이터보호이사회는 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 유럽 데이터보호이사회에 의견을 요청하지 않거나 제64조로 발부된 유럽 데이터보호이사회의 의견에 따르지 않을 경우. 이 같은 경우, 관련 감독기관이나 집행위원회는 유럽 데이터보호이사회에 해당 사안을 전달할 수 있다.

2. 제1항에 명시된 결정은 유럽 데이터보호이사회 위원의 2/3 다수결에 의해 사안의 상정 후 1개월 이내에 채택되어야 한다. 이 기간은 사안의 복잡성을 감안하여 1개월간 추가 연장될 수 있다. 제1항에 명시된 결정은 타당하고 선임 감독기관과 모든 관련 감독기관을 대상으로 해야 하며 이들에게 구속력을 가져야 한다.

3. 유럽 데이터보호이사회는 제2항에 명시된 기간 내에 결정문을 채택할 수 없을 경우, 제2항에 명시된 두 번째 달의 만료 후 2주 이내에 위원회 단순 다수결로 결정문을 채택해야 한다. 이사회 위원들이 분열될 경우, 의장의 의결로 결정문을 채택해야 한다.

4. 관련 감독기관은 제2항 및 제3항에 명시된 기간 동안 제1항에 따라 유럽 데이터보호이사회에 제출된 사안에 대하여 결정을 채택해서는 안 된다.

5. 유럽 데이터보호이사회 의장은 제1항에 명시된 결정을 부당한 지체 없이 관련 감독기관에게 통보해야 한다. 집행위원회에도 통보해야 한다. 감독기관이 제6항에 명시된

최종 결정을 통보한 후 이는 지체 없이 유럽 데이터보호이사회 웹사이트에 게재되어야 한다.

6. 선임 감독기관 또는 경우에 따라 민원을 접수한 감독기관은 제1항에 명시된 결정을 근거로 부당한 지체 없이, 늦어도 유럽 데이터보호이사회가 결정을 게재한 후 1개월 이내에 최종 결정을 채택해야 한다. 선임 감독기관 또는 경우에 따라 민원을 접수한 감독기관은 최종 결정이 컨트롤러나 프로세서 및 정보주체에 각각 고지되는 날짜를 유럽 데이터보호이사회에 통보해야 한다. 관련 감독기관들의 최종 결정은 제60조(7), (8) 및 (9)항의 조건으로 채택되어야 한다. 최종 결정은 제1항에 명시된 결정을 지칭하며, 제5항에 따라 유럽 데이터보호이사회 웹사이트에 제1항의 결정이 게재될 것임을 명시해야 한다. 최종 결정에는 제1항에 명시된 결정이 첨부되어야 한다.

제66조

긴급성(시급성) 절차

1. 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 기간을 지정하여 즉시 채택할 수 있다. 감독기관은 지체 없이 해당 조치 및 조치의 채택 사유를 나머지 감독기관, 유럽 데이터보호이사회 및 집행위원회에 전달해야 한다.

2. 감독기관이 제1항에 따른 조치를 취하고 최종 조치를 시급히 채택해야 한다고 판단할 경우, 유럽 데이터보호이사회에 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 유럽 데이터보호이사회에 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 조 제2항 및 제3항에 명시된 긴급한 의견이나 법적 구속력이 있는 결정은 2주 이내에 이사회 위원들의 단순 다수결로 채택되어야 한다.

제67조

정보의 교환

1. 집행위원회는 감독기관들 간, 그리고 감독기관과 유럽 데이터보호이사회 간에 제64조에

명시된 표준화된 양식 등 전자적 수단으로 정보를 교환하기 위한 방식을 규정하기 위해 일반적 범위의 이행 법률을 채택할 수 있다.

그 같은 이행 법률은 제93조(2)에 명시된 검토절차에 따라 채택되어야 한다.

제3절
유럽 데이터보호이사회

제68조
유럽 데이터보호이사회

1. 유럽 데이터보호이사회(이사회)를 유럽연합 기구로 정하고 법인격을 가지도록 한다.

2. 이사회는 의장이 대표한다.

3. 이사회는 각 회원국 감독기관의 장과 유럽 데이터보호 감독기구(European Data Protection Supervisor), 또는 각 대리인으로 구성된다.

4. 한 회원국에서 하나 이상의 감독기관이 본 규정에 따른 조문의 적용을 모니터링 할 책임이 있는 경우, 해당 회원국의 법률에 따라 공동 대리인이 임명되어야 한다.

5. 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, 유럽 데이터보호 감독기구는 유럽연합 산하기관, 기구, 사무소 및 에이전시에 적용되고 사실상 본 규정에 상응하는 원칙 및 규정에 관한 결정에 대해서만 의결권을 갖는다.

제69조
독립성

1. 유럽 데이터보호이사회는 제70조 및 제71조에 따른 임무를 수행하거나 권한을 행사할 때 독립적으로 활동한다.

2. 제70조(1) (b)호 및 제70조(2)에 명시된 집행위원회의 요청을 침해하지 아니하여, 유럽 데이터보호이사회는 임무를 수행하거나 권한을 행사하는 중에 다른 어느 누구로부터도 지시를 구하거나 그들의 지시를 따르지 아니한다.

제70조

유럽 데이터보호이사회의 업무

1. 유럽 데이터보호이사회는 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 컨트롤러, 프로세서, 감독기관 간에 이루어지는 정보 교환의 양식 및 절차에 대해 집행위원회에 자문을 제공한다.

(d) 제17조(2)에 명시된 대로 일반에 공개되는 통신 서비스로부터 개인정보의 링크, 사본 또는 복제본을 삭제하기 위한 절차에 대해 가이드라인, 권고사항 및 모범사례를 발행한다.

(e) 자발적으로 또는 소속 위원의 요청에 따라 또는 집행위원회의 요청에 따라 본 규정의 적용에 대한 질의사항을 검토하고 본 규정의 일관적 적용을 장려하기 위해 가이드라인, 권고사항 및 모범사례를 발행한다.

(f) 제22조(2)에 따른 프로파일링을 기반으로 하는 결정의 기준 및 조건을 추가로 명시하기 위해 본 항 (e)호에 부합하는 가이드라인, 권고사항 및 모범사례를 발행한다.

(g) 개인정보 침해를 규명하고 제33조(1) 및 (2)항에 명시된 부당한 지체를 결정하기 위해서, 그리고 컨트롤러 또는 프로세서가 개인정보 침해에 대해 고지해야 하는 특정 상황에 대하여 본 항 (e)호에 부합하는 가이드라인, 권고사항 및 모범사례를 발행한다.

(h) 개인정보 침해가 제34조(1)에 명시된 개인의 권리와 자유에 대한 중대한 위험을 초래할 가능성이 있는 상황에 대해 본 항 (e)호에 부합하는 가이드라인, 권고사항 및 모범사례를 발행한다.

(i) 컨트롤러가 준수하는 의무적 기업 규칙과 프로세서가 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 항 (e)호에 부합하는 가이드라인, 권고사항 및 모범사례를 발행한다.

(j) 제49조(1)을 근거로 하는 개인정보 이전에 대한 기준 및 요건을 추가로 명시하기 위해

본 항 (e)호에 부합하는 가이드라인, 권고사항 및 모범사례를 발행한다.

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

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

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

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

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

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

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

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

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

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

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

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

(w) 전 세계 데이터보호 감독기관들과의 데이터보호 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 유럽 데이터보호이사회의 자문을 요청하는 경우, 사안의 시급성을 감안하여 시한을 명시할 수 있다.

3. 유럽 데이터보호이사회는 집행위원회와 제93조에 명시된 위원회(committee)에 이사회의 의견, 가이드라인, 권고사항 및 모범사례를 전달해야 한다.

4. 유럽 데이터보호이사회는 적절한 경우 이해당사자와 협의하고 적정한 기간 내에 의견을 개진할 기회를 제공해야 한다. 이사회는 제76조를 침해하지 않고 협의 절차의 결과를 공개해야 한다.

제71조

보고서

1. 유럽 데이터보호이사회는 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)조 (l)호에 명시된 가이드라인, 권고사항과 모범사례 및 제65조에 명시된 법적 구속력이 있는 결정의 실제 적용에 관한 검토가 포함되어야 한다.

제72조

절차

1. 유럽 데이터보호이사회는 본 규정에서 별도로 규정하지 않는 한 이사회 위원의 단순 다수결로 결정을 내린다.

2. 유럽 데이터보호이사회는 위원의 2/3 다수결로 자체적인 절차 규정을 채택하고 자체적인 운영 방식을 조직한다.

제73조

의장

1. 유럽 데이터보호이사회는 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) 유럽 데이터보호이사회 회의를 소집하고 안건을 준비한다.

(b) 제65조에 의거하여 유럽 데이터보호이사회가 채택한 결정을 선임 감독기관 및 관련 감독기관에 통보한다.

(b) 특히 제63조의 일관성 메커니즘과 관련해 유럽 데이터보호이사회의 업무가 적시에 수행되도록 한다.

2. 유럽 데이터보호이사회는 이사회의 절차 규정에 의장과 부의장 간의 업무 분장을 규정해야 한다.

제75조

사무국

1. 유럽 데이터보호이사회는 유럽 데이터보호 감독기구가 제공하는 사무국을 둔다.

2. 사무국은 이사회 의장의 지시에 따라 독자적으로 업무를 수행한다.

3. 본 규정이 유럽 데이터보호이사회에 부여한 업무를 수행하는데 관여하는 유럽 데이터보호 감독기구의 직원은 유럽 데이터보호 감독기구에 부여된 업무의 수행에 관여하는 직원과 별도의 보고 체계를 따라야 한다.

4. 적절한 경우, 유럽 데이터보호이사회와 유럽 데이터보호 감독기구는 본 조문을 이행하는 양해각서를 체결 및 발표해야 한다. 양해각서는 협력 조건을 결정하고 본 규정이 유럽 데이터보호이사회에 부여한 업무를 수행하는데 관여하는 유럽 데이터보호 감독기구 직원에 적용된다..

5. 사무국은 유럽 데이터보호이사회에 분석적, 행정적, 로지스틱 관련 지원을 제공해야 한다.

6. 사무국은 특히 다음에 대한 책임이 있다.

(a) 유럽 데이터보호이사회의 일일 업무

(b) 유럽 데이터보호이사회 위원들, 의장 및 유럽 집행위원회 간의 소통

(c) 기타 기구 및 일반과의 소통

(d) 내·외부 소통을 위한 전자적 수단 활용

(e) 관련 정보의 번역

(f) 유럽 데이터보호이사회 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. 유럽 데이터보호이사회는 절차 규정에 규정된 바와 같이 필요하다고 판단하는 경우 이사회의 논의를 기밀로 해야 한다.

2. 유럽 데이터보호이사회 위원, 전문가 및 제3자의 대리인에게 제출된 문서의 열람은 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 유럽 데이터보호이사회의 의견이나 결정에 이은 감독기관의 결정에 대하여 법적 절차가 제기될 경우, 감독기관은 그 의견이나 결정을 법원에 전달해야 한다.

제79조

컨트롤러나 프로세서를 상대로 한 효과적인 사법구제권

1. 제77조에 따른 감독기관에 민원을 제기할 권리 등 가용할 수 있는 행정적 또는 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. 컨트롤러 또는 프로세서를 상대로 한 법적 절차는 해당 컨트롤러 또는 프로세서의 사업장이 있는 회원국의 법정에서 진행되어야 한다. 그렇지 않으면 컨트롤러 또는 프로세서가 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, 본 조 제1항에 명시된 기구, 조직 또는 협회가 정보주체의 권한과 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 컨트롤러나 프로세서의 개인정보 처리에 대하여 동일한 사안의 법적 절차에 관한 정보를 가지고 있는 경우, 그 회원국의 법원에 연락하여 해당 법적 절차의 존재 유무를 확인해야 한다.

2. 동일 컨트롤러나 프로세서의 데이터 처리에 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 컨트롤러 또는 프로세서로부터 피해 보상을 받을 권리가 있다.

2. 데이터 처리에 관여하는 컨트롤러는 본 규정을 침해하는 정보처리로 초래된 피해에 대하여 책임을 져야 한다. 프로세서는 프로세서들에게 구체적으로 지시된 본 규정의 의무사항을 준수하지 않은 경우 또는 컨트롤러의 합법적 지시를 벗어나거나 그 지시에 반대되는 행동을 한 경우에 한하여 데이터 처리로 초래된 피해에 대하여 책임을 져야 한다.

3. 피해를 초래한 사건에 대하여 어떠한 식으로도 책임이 없음을 증명할 경우, 컨트롤러 또는 프로세서는 제2항에 의거한 책임에서 면제된다.

4. 하나 이상의 컨트롤러 또는 프로세서가 동일한 데이터 처리에 관여하고 제2항 및 제3항에 따라 해당 데이터 처리로 초래된 피해에 대하여 책임이 있는 경우, 각 컨트롤러나 프로세서는 정보주체의 유효한 보상을 보장하기 위해 피해 전체에 대하여 책임을 져야

한다.

5. 컨트롤러 또는 프로세서가 제4항에 따라 피해에 대해 전액 보상한 경우, 해당 컨트롤러 또는 프로세서는 제2항에 명시된 조건에 부합하여 동일한 데이터 처리에 관여한 기타 컨트롤러나 프로세서에게 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 제4항, 제5항 및 제6항에 명시된 본 규정의 침해와 관련하여, 본 조문에 따른 행정 과태료의 부과가 개별 사례에서 유효하고 비례적이며 (침해행위를 하지 않도록 하는) 설득력이 있도록 해야 한다.

2. 행정 과태료는 각 개별 사례의 정황에 따라 제58조(2)의 (a)-(h)호 및 (j)호에 언급된 조치에 추가로 부과되거나 그 대신 부과되어야 한다. 각 개별 사례에서 행정 과태료 부과 여부를 결정하거나 행정 과태료 액수를 결정할 때 다음 사항을 면밀히 고려해야 한다.

(a) 관련 데이터 처리의 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 컨트롤러나 프로세서가 취한 조치

(d) 제25조 및 제32조에 의거하여 컨트롤러 또는 프로세서가 이행한 기술 및 관리적 대책을 고려한 컨트롤러 또는 프로세서의 책임의 정도

(e) 컨트롤러 또는 프로세서의 이전의 관련 침해건

(f) 침해를 구제하고 침해의 악영향을 완화하기 위한 감독기관과의 협력 수준

(g) 침해로 영향을 받은 개인정보의 범주

(h) 컨트롤러 또는 프로세서가 침해를 통보했는지 여부 및 그런 경우 통보의 정도 등 침해 사실이 감독기관에 알려지게 된 방식

(i) 동일한 사안에 대하여 관련 컨트롤러나 프로세서에 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. 컨트롤러나 프로세서가 의도적으로 또는 부주의하여 동일하거나 연계된 데이터 처리 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 제2항에 따라 10 000 000 유로에 이르는 행정 과태료 또는 사업체의 경우 직전 회계연도의 연간 전 세계 총 매출의 2%에 이르는 행정 과태료 중 높은 금액의 처분을 받는다.

(a) 제8, 11, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 42조 및 제43조에 따른 컨트롤러 및 프로세서의 의무

(b) 제42조 및 제43조에 따른 인증기관의 의무

(c) 제41조(4)에 따른 모니터링 기관의 의무

5. 다음과 같은 조문의 침해는 제2항에 따라 20 000 000 유로에 이르는 행정 과태료 또는 사업체의 경우 직전 회계연도의 연간 전 세계 총 매출의 4%에 이르는 행정 과태료 중 높은 금액의 처분을 받는다.

(a) 제5조, 제6조, 제7조 및 제9조에 따른 동의 조건을 비롯한 데이터 처리의 기본 원칙

(b) 제12조-제22조에 따른 정보주체의 권리

(c) 제44조-제49조에 따른 제3국이나 국제기구의 수령인에게로의 개인정보 이전

(d) IX장에 따라 채택된 회원국 법률에 따른 의무

(e) 제58조(2)에 따라 감독기관이 내린 명령, 또는 데이터 처리의 한시적 또는 확정적 제한, 또는 개인정보 이동의 중지를 준수하지 않거나 열람의 기회를 제공하지 않아 제58조(1)를 위반

6. 제58조(2)에 명시된 바와 같이 감독기관의 명령 불복은 제2항에 따라 20 000 000 유로에 이르는 행정 과태료 또는 사업체의 경우 직전 회계연도의 연간 전 세계 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 2018년 5월 25일까지, 그리고 지체 없이 본 항에 따라 채택하는 자국법의 조문을 집행위원회에 통보하고, 이에 영향을 미치는 차후의 개정법이나 개정안을 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 2018년 5월 25일까지, 그리고 지체 없이 제1항에 따라 채택하는 자국법의 조문을 집행위원회에 통보하고 이에 영향을 미치는 차후의 개정안을 집행위원회에 통보해야 한다.

제IX장

특정 처리 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(컨트롤러 및 프로세서), 제5장(제3국 또는 국제기구로의 개인정보 이전), 제6장(독립적 감독기관), 제7장(협력 및 일관성), 제9장(특정 데이터 처리상황)의 면제 또는 적용 일부 제외를 규정해야 한다.

3. 각 회원국은 제2항에 따라 채택한 자국법의 조문과 이에 영향을 미치는 차후의 개정법 또는 개정안을 지체 없이 집행위원회에 통보해야 한다.

제86조

개인정보 처리 및 공식 문서 공개

공공당국, 공공기관 또는 민간기관가 공익을 위해 실시하는 업무의 수행을 위해 보유하고 있는 개인정보는 본 규정에 따른 공식 문서의 일반 공개와 개인정보 보호권 사이의 균형을 유지시키기 위해 유럽연합 법률 또는 해당 공공당국이나 기관에 적용되는 회원국 법률에 의거하여 해당 기관이나 기구가 공개할 수 있다.

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 처리

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 평등과 다양성, 작업 중의 건강과 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 데이터 처리의 투명성과 공동 경제활동에 종사하는 사업체 또는 기업 집단 내에서 이루어지는 데이터 이전, 직장에서의 모니터링 시스템과 관련하여 정보주체의 존엄성과 정당한 이익 및 기본권을 보호하는데 적절하고 구체적인 대책이 포함되어야 한다.

3. 각 회원국은 2018년 5월 25일까지, 그리고 지체 없이 제1항에 따라 채택하는 자국법의 조문을 집행위원회에 통보하고, 이에 영향을 미치는 차후의 개정안을 집행위원회에 통보해야 한다.

제89조

공익적 기록보존 목적, 과학적 또는 역사적 연구 목적, 또는 통계적 목적을 위한 처리와 관련한 안전조치 및 적용의 일부 제외

1. 공익적 기록보존 목적, 과학적 또는 역사적 연구 목적, 또는 통계적 목적을 위한 처리는 정보주체의 권리 및 자유를 위해 본 규정에 따라 적정한 안전조치가 적용되어야 한다. 그러한 안전조치는 특히 데이터 최소화 원칙이 준수되도록 기술 및 관리적 조치를 이행해야 한다. 그러한 조치에는 가명처리 방식으로 그러한 목적들을 달성할 수 있다면 가명처리가 포함될 수 있다. 정보주체의 식별을 허용하지 않거나 더 이상 허용하지 않는 추가 처리를 통해 그러한 목적들을 달성될 수 있는 경우에는 그러한 방식으로 달성되어야 한다.

2. 개인정보가 과학적 또는 역사적 연구 목적이나 통계적 목적으로 처리되는 경우, 유럽연합 또는 회원국 법률은 본 조 제1항의 조건 및 안전조치에 따라 제15조, 제16조, 제18조 및 제21조에 규정된 권리의 적용을 일부 제외할 수 있다. 단, 그러한 권리가 그러한 특정 목적의 달성을 불가능하게 하거나 중대하게 손상시킬 것으로 예상되고, 그러한 목적을 달성하기 위하여 적용의 일부 제외가 필요한 것이어야 한다.

3. 공익을 위한 기록보존의 목적으로 개인정보가 처리되는 경우, 유럽연합 또는 회원국 법률은 제15조, 제16조, 제18조, 제19조, 제20조 및 제21조에 명시되고 본 조 제1항의 조건 및 안전조치에 따른 권리로 인해 특정 목적의 달성을 불가능하게 하거나 중대하게 손상시킬 것으로 예상되고, 적용의 일부 제외가 해당 목적을 달성하기 위해 요구되는 한, 해당 권리의 적용을 일부 제외하도록 규정할 수 있다.

4. 제2항 및 제3항에 명시된 정보처리가 동시에 다른 목적으로 이루어지는 경우, 적용의 일부 제외는 해당 호에 명시된 목적을 가진 데이터 처리에만 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 컨트롤러나 프로세서와 관련하여 제58조(1) (e)호 및 (f)호에 규정된 감독기관의 권한을 규정하는 특정 규칙(rules)들을 채택할 수 있다. 그러한 규칙은 해당 기밀유지의 의무가 적용되는 활동의 결과로 또는 활동 중에 컨트롤러나 프로세서가 입수한 개인정보에 한하여 적용되어야 한다.

2 각 회원국은 2018년 5월 25일까지, 그리고 지체 없이 제1항에 따라 채택하는 자국법의 조문을 집행위원회에 통보하고, 이에 영향을 미치는 차후의 개정안을 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. 제1항에 따라 포괄적인 규칙을 적용하는 교회 및 종교 단체는 독립적 감독기관의 통제를 받게 되고 이는 구체적일 수 있다. 단, 이로써 본 규정의 제6장이 정한 조건이 충족되는 경우에 그러하다.

제X장

위임법률 및 이행법률

제92조

위임의 행사

1. 본 조문에 규정된 조건에 따라 집행위원회는 위임법률을 채택할 수 있는 권한을 부여받는다.

2. 제12조(8) 및 제43조(8)에 명시된 권한의 위임은 2016년 5월 4일로부터 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. 결정은 유럽연합 관보에 게재된 다음 날 또는 거기에 지정된 차후의 날짜에 발효된다. 결정은 이미 발효 중인 위임법률의 유효성(효력)에는 영향을 미쳐서는 아니 된다.

4. 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 항을 참조하는 경우, 규정서 (EU) No 182/2011의 제5조가 적용되어야 한다.

3. 본 항을 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 2018년 5월 25일부터 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 유럽 데이터보호이사회에 대한 참조로 해석되어야 한다.

제95조

지침 2002/58/EC와의 관계

본 규정은 유럽연합 역내의 공공 통신 분야에서 공용의 전자 통신 서비스를 제공하는 것과 관련해 개인 또는 법인이 지침 2002/58/EC에 규정된 동일한 목적의 특정 의무를 따라야 하는 사안에 대하여 그들에게 추가적 의무를 부과해서는 아니 된다.

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 2020년 5월 25일까지, 그리고 이후 매 4년마다, 본 규정의 평가 및 검토에 관한 보고서를 유럽의회 및 각료이사회에 제출해야 한다. 보고서는 공개되어야 한다.

2. 제1항에 명시된 평가 및 검토를 할 때 집행위원회는 특히 다음 사항의 적용 및 기능을 면밀히 검토해야 한다.

(a) 특히 본 규정의 제45조(3)에 따라 채택되는 결정 및 지침 95/46/EC의 제25조(6)을 근거로 채택되는 결정과 관련하여 제3국이나 국제기구로의 개인정보 이전에 대해 규정한 제5장

(b) 협력 및 일관성에 관한 제7장

3. 제1항의 목적을 위하여, 집행위원회는 회원국과 감독기관에 정보를 요청할 수 있다.

4. 집행위원회는 제1항 및 제2항의 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 에이전시의 데이터 처리와 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 2018년 5월 25일부터 적용된다.

본 규정은 전체로서 법적 구속력을 가지며 모든 회원국들에 직접적으로 적용 가능해야 한다.

유럽의회 의장

유럽각료이사회 의장