World Economy Today

KIEP
오늘의 세계경제

Korea Institute for International Economic Policy

2018년 5월 25일 Vol. 18 No. 19

ISSN 1976-0515

EU 개인정보보호법(GDPR) 발효: 평가 및 대응방안

오태현 세계지역연구센터 선진경제실 구미팀 전문연구원 (asroc101@kiep.go.kr, Tel: 044-414-1159)

강민지 무역통상실 무역협정팀 연구원 (mjkang@kiep.go.kr, Tel: 044-414-1196)

KIEP 대외경제정책연구원 Korea Institute for International Economic Policy

30147 세종특별자치시 시청대로 370 세종국책연구단지 경제정책동
T.044-414-1114 F.044-414-1001 • www.kiep.go.kr

차 례

주요 내용

▶ 2018년 5월 25일 EU의 개인정보보호법(GDPR: General Data Protection Regulation)이 발효

- EU GDPR은 디지털 단일시장전략을 통해 공동의 혁신기반을 구축하고, 회원국 간 자유로운 정보이동을 장려하고 개인정보주체자의 권리 및 책임자의 의무를 강화하는 데 목적이 있음.

▶ 정보의 중요성이 점차 강조되는 디지털 경제에서 EU GDPR은 개인정보보호에 관한 선도적인 규제안을 제시

- [적용대상 범위 확대] 기존에는 EU에 사업장을 운영하며 개인정보 처리를 수반하는 경우로 제한되었으나, GDPR에서는 EU 밖에서 ① EU에 있는 정보주체에게 재화나 서비스를 제공하거나, ② EU 내에 있는 정보주체의 활동을 모니터링하는 경우로 확대됨(제3조).
- [정보주체 권리 강화] 정보사회의 발전에 대응하여 EU 지침(Directive 95/46/EC)에는 없던 삭제권(잊혀질 권리), 처리제한권, 정보이전권이 새롭게 도입되어 정보주체의 권리가 강화됨.
- [컨트롤러와 프로세서의 책임 강화] GDPR은 개인정보보호와 관련하여 컨트롤러와 프로세서의 책임을 강화하기 위해 개인정보 처리 활동을 서면으로 관리·보관해야 함.
- [개인정보의 역외이전] EU 역외로 개인정보를 이전하는 경우, GDPR은 ① 제3국이 적정성 결정 승인을 획득한 경우이거나, ② 개인정보를 이전하려는 기업이 적절한 보호조치를 갖춘 경우로 제한됨.

▶ EU GDPR은 단기적으로 새로운 인프라 구축, 인력양성 및 조직개편, 정보를 활용한 혁신적인 중소벤처 스타트업 출범의 어려움 등 사회경제적 비용을 유발할 수 있으나, 중장기적으로 개인정보보호 강화에 따른 소비자 신뢰 증가와 국경 간 좀 더 자유로운 정보이동이라는 측면에서 사회경제적 편익이 더 클 수 있을 것으로 판단

▶ EU GDPR은 개인정보보호 수준 강화 및 자유로운 정보이동 촉진 측면에서 디지털 시대에 가장 포괄적이며 미래지향적인 입법으로 향후 개인정보보호에 관한 글로벌 표준 정립에 영향을 미칠 것으로 판단

▶ 한국정부는 EU GDPR을 계기로 국내 개인정보보호 법제상 개인정보보호와 활용의 균형을 맞추기 위한 개선 노력이 요구되며, 현재 심의 중인 EU 집행위원회의 '적정성 결정(adequacy decisions)'이 빨리 승인될 수 있도록 정부 차원의 적극적인 협상과 지원이 요구

▶ 한국기업들은 EU GDPR이 요구하는 의무사항을 준수할 수 있도록 기업 차원의 조직개편 및 대응전략 수립이 요구되며, 동시에 EU GDPR 대응을 통해 개인정보보호에 관한 소비자 신뢰를 제고하고 합법적·효과적으로 정보를 활용하는 기회로 인식하는 것이 필요

1. EU GDPR의 개요

■ 2018년 5월 25일 EU의 개인정보보호법(GDPR: General Data Protection Regulation)이 발효됨.[1)]

- EU GDPR은 4년간의 공론화 과정을 거쳐 지난 2016년 5월에 규정(Regulation)으로 제정되었으며, 기존 EU의 1995년 개인정보보호지침(Directive)을 대체함(부록 표 1 참고).[2)]
  - ○ 개인정보보호는 EU 기능조약(TFEU: Treaty on the Functioning of the European Union) 제16조 및 EU 기본헌장(Charter of Fundamental Rights of the European Union) 제8조를 기반으로 함.
- 1995년 EU 개인정보보호지침(Directive 95/46/EC, 이하 EU 지침)은 개인정보보호라는 공통의 목적에도 불구하고 새로운 기술의 도입, 국별로 상이한 제도기반과 법적 환경 등에 따라 EU 회원국 간 자유로운 정보의 이동을 제한하고, EU가 목표로 하는 단일시장의 발전을 저해하는 요인으로 작용[3)]
  - ○ 개인정보의 회원국 간 이동을 위해 요구되는 정보보호 당국의 등록 또는 허가 기준이 서로 상이하고, 일부 회원국은 개인정보보호에 관한 법률이 부재함.
  - ○ 또한 1995년 이후 새로운 기술이 개발됨에 따라 기존 법체제로는 충분히 개인정보를 보호하기 어렵다는 평가가 있음.
- 2012년 GDPR 초안이 처음 발표된 이후 4,000번이 넘는 수정이 이루어졌으며, 유럽의회 역사에서 가장 많은 로비가 이루어진 법안으로 기록됨.[4)]

■ EU는 디지털 단일시장전략을 통해 회원국 간 정보이동을 자유롭게 하고 공동의 혁신기반을 구축하고자 정책적인 노력을 하고 있으며, 디지털 경제에서 정보의 중요도가 제고됨에 따라 정보보호의 중요성이 강조됨.

- 독일 연구기관이 EU 시민들을 대상으로 실시한 설문조사에서 다수의 응답자들은 자신들이 온라인상 개인정보에 대한 완전한 통제권을 갖고 있지 못하다고 밝힘.
  - ○ 2015년에 조사에서 평균적으로 10명 중 8명이 온라인에 제공하는 개인정보에 대한 통제에 우려를 나타냄(그림 1 참고).
- 반면 정보를 활용하는 기업은 2017년 기준으로 약 69만 개의 법인이나 단체가 개인정보를 활용하고 있으며, 그 수는 계속 증가할 것으로 전망됨.
  - ○ IDC와 The Lisbon Council이 발표하는 유럽정보시장 조사에 따르면, 2017년 기준 EU 역내에서 개인정보를 활용하는 법인과 단체는 690,650개로 전년대비 2.1%가 증가했으며, 2020년까지 721,850개로 증가할 전망임(그림 2 참고).
  - ○ 산업 부문별로는 전문서비스 분야의 개인정보 사용이 가장 높게 나타났으며, 다음으로 제조업, 교통, ICT 순임.

---

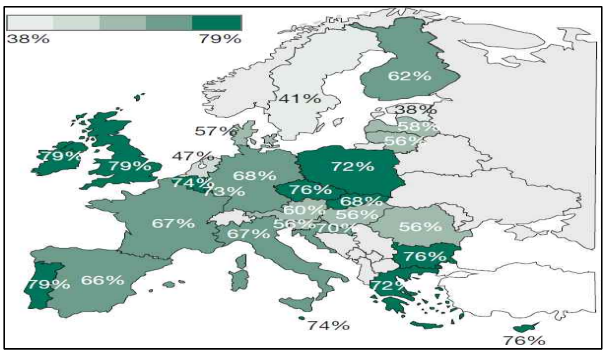
1) 규정(Regulation)은 별도의 국내입법 과정 없이 회원국에 직접적으로 적용되는 EU법인 반면, 지침(Directive)은 법적용을 위해서 회원국별 별도의 국내입법과정이 요구됨. 동 보고서에서는 이해의 제고를 위해 EU법상의 공식 명칭인 "개인정보보호규정" 대신 "개인정보보호법"으로 지칭함.

2) European Union(2016), *Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*; European Union. 1995. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.*

3) 당초 EU 집행위가 새로운 개인정보보호 법안을 논의하는 시점에서 규정이 기존 지침을 대체할 것이라는 명확한 의도가 있었는지는 불분명함. European Commission(2010), *A Comprehensive Approach on Personal Data Protection in the European Union.*

4) European Commission(2013), "LIBE Committee Vote Backs New EU Data Protection Rules."

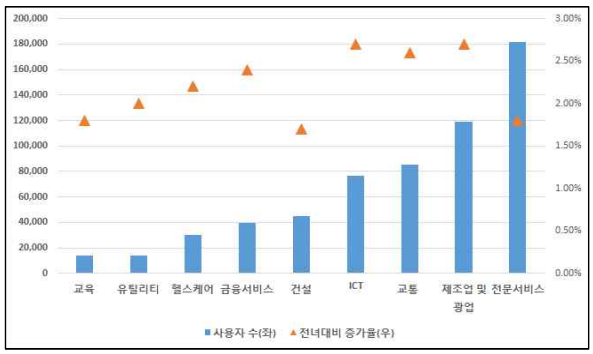
그림 1. 당신은 온라인상 개인정보에 대한 완전한 통제권을 갖고 있지 못하다고 생각하는가?(2015년)



자료: ZBW(2017).

그림 2. EU 산업 부문별 정보 사용자(2017년)

(단위: 개, %)



주: 데이터 사용자는 데이터를 활용하는 EU 역내 법인 및 단체를 의미.
자료: IDC and The Lisbon Council(2018).

■ GDPR은 EU 역내에 거주하는 자연인의 개인정보를 필요로 하는 모든 기업을 대상으로 하며, 무엇보다 규정 위반에 따른 벌금규모가 크다는 점이 특징임(표 1 참고).

- 개인정보를 수집하거나 다른 기업을 위해 정보를 처리하는 기업이 모두 GDPR의 적용대상이 됨.
  - ○ 개인정보에는 자연인의 이름, 주소, 위치(지역), 온라인 식별정보(IP), 건강정보, 소득, 문화정보 등이 포함됨.
  - ○ GDPR은 EU 역내외 모든 기업을 대상으로 하고 있다는 점에서 일명 '브뤼셀 효과'로 불리는 강력한 규제에 해당됨.
- GDPR의 입법 전 과정을 담당했던 제29조 작업반(Article 29 Working Party)은 GDPR의 발효와 함께 유럽 개인정보보호이사회(EDPB: European Data Protection Board)로 대체되며, 유럽의 개인정보에 관한 정책자문을 계속해서 지원하게 됨.[5)]
  - ○ 제29조 작업반은 개인정보보호를 위한 EU의 자문기구로 1995년 개인정보보호지침의 제29조에 기반하여 1996년에 설립됨.

표 1. EU GDPR의 주요 특징

항목	주요 특징
적용 범위	• 설립지와 상관없이 EU 역내에 거주하는 자연인의 개인정보를 처리하는 컨트롤러 및 프로세서 • 역외 기업의 경우 EU 역내 대리인 지정(의무사항)
보호 강화	• 개인정보의 범위가 확대되어, IP 주소, 쿠키, RFID 등이 온라인 식별자에 포함 • 개인정보에 대한 동의, 접근, 프로파일링, 정보이동 등에 새로운 규제 적용 • 6가지 원칙: 적법성·공정성·투명성, 목적 제한, 개인정보 최소화, 정확성, 저장 제한, 무결성·기밀성
원스톱 숍	• 개인정보보호 강화를 위한 European Data Protection Board 설립 • 주사업장 또는 단일사업장의 선임감독기관이 컨트롤러와 프로세서를 감독
제재 강화	• 심각한 위반에 대해 2천만 유로까지 과징금 또는 직전 전 세계 매출액의 4%까지 과징금 중 큰 금액 • 일반적 위반에 대해 1천만 유로까지 과징금 또는 직전 전 세계 매출액의 2%까지 과징금 중 큰 금액
정보주체의 권리 강화	• 정보 유출에 따른 피해가 발생할 경우 보상청구 가능 • '잊혀질 권리(삭제권)', '처리제한권', '정보이전권' 새롭게 도입
개인정보 유출 시 대응	• 컨트롤러는 개인정보가 유출된 사실을 알게 된 시점으로부터 72시간 이내에 감독당국에 신고 • 정보주체에게 고위험이 예상되는 경우 지체 없이 정보주체에게도 고지

주: 컨트롤러와 프로세서에 대한 정의는 본 보고서의 제2장 EU GDPR의 주요 내용을 참고.
자료: European Commission(2016) 자료 활용하여 저자 작성.

5) Directive 95/46/EC Article 29. Working Party on the Protection of Individuals with regard to the Processing of Personal Data.

2. EU GDPR의 주요 내용

■ [개요 및 목적] GDPR은 자연인에 대한 개인정보보호권을 담보하고(제1조 제2항), EU 역내에서 개인정보의 자유로운 이동을 보장(제1조 제3항)하는 것을 목적으로 함.

- GDPR은 상설(Recital) 총 173개조, 본문 총 11장 및 99개조로 이루어져 기존 EU 지침이 상설 총 72개조, 본문 총 7장 및 34개조로 이루어진 것에 비해 조문 수가 대폭 증가함(표 2 참고).
- GDPR은 2018년 5월 25일부터 기존 EU 지침을 대체하며 법적 구속력을 가지고 EU 모든 회원국에 직접적으로 적용됨(제99조).

○ 단, 일부 규정은 회원국의 별도 입법이 요구됨.[6)]

표 2. GDPR의 구성

상설(Recital) 173개	
본문 11장 99개 조항	제1장 일반규정(General Provision)
	제2장 원칙(Principles)
	제3장 정보주체의 권리(Rights of the Data Subject)
	제4장 컨트롤러와 프로세서(Controller and Processor)
	제5장 제3국 및 국제기구로의 개인정보 이전 (Transfer of Personal Data to Third Countries of International Organizations)
	제6장 독립적인 감독기구(Independent Supervisory Authorities)
	제7장 협력 및 일관성(Co-operation and Consistency)
	제8장 권리구제, 책임 및 제재(Remedies, Liability and Sanctions)
	제9장 특정정보 처리 상황에 관한 규정(Provisions Relating to Specific Data Processing Situations)
	제10장 위임법률 및 시행법률(Delegated Acts and Implementing Acts)
	제11장 최종규정(Final Provisions)

■ [적용대상] GDPR은 살아 있는 자연인의 개인정보[7)]에 적용됨.

- GDPR은 개인정보의 처리에 적용되나, 익명으로 처리되어 더 이상 식별될 수 없는 익명정보에는 GDPR이 적용되지 않음에 따라 기업들은 해당 정보를 분석함으로써 기업 비즈니스에 활용할 수 있음.
- GDPR은 인종·민족, 정치적 견해, 종교·신념, 노동조합 가입여부, 유전정보, 건강, 성생활 또는 성적 취향 등의 민감정보를 '특별한 유형(special categories)의 개인정보'로 규정하여 정보주체의 명시적 동의가 없이는 원칙적으로 처리를 금지하고 있음(제9조 제1항).

■ [적용범위] EU에 사업장을 운영하며 개인정보 처리를 수반하는 경우에 더하여, ① EU 밖에서 EU에 있는 정보주체에게 재화나 서비스를 제공하거나, ② EU 내에 있는 정보주체의 활동을 모니터링하는 경우에도 적용됨(제3조).

6) 예를 들어 과징금의 대상이 되지 않는 위반사항에 대해 각 회원국이 처벌에 관한 별도의 입법을 하여야 함(제84조 제1항).
7) 개인정보(personal data): 식별되었거나 또는 식별가능한 자연인(정보주체)과 관련된 모든 정보를 의미함. 자연인을 직·간접적으로 식별 가능한 경우라면 이름·전화번호 등과 같은 일반적인 개인정보 외에 EU 지침에는 포함되지 않았던 위치정보, IP 주소 등 온라인 식별자 정보도 개인정보에 해당함(제4조).

- ①, ②의 경우 개인정보가 처리되는 정보주체가 거주하는 회원국들 중 하나에 대리인을 지정하여야 함.
- EU에 설립되어 있지 않아도 EU에 거주하는 자연인에게 재화 및 서비스를 제공하는 목적이 분명한 한국기업은 GDPR의 적용을 받으며, 이때 제공되는 서비스의 언어, 통화, 서비스 제공대상 등이 고려됨.
  - 예를 들어, 한국에서 운영되는 웹사이트가 EU 회원국인 독일의 통화(화폐)와 언어를 지원하고, 독일에 상품을 배송하는 국제 배송서비스를 제공하는 경우 GDPR이 적용될 수 있음.

■ **[주요 원칙] ① 처리의 적법성·공정성·투명성 원칙, ② 수집 목적 제한의 원칙, ③ 개인정보처리 최소화 원칙, ④ 정확성 원칙, ⑤ 보관 기간 제한의 원칙, ⑥ 무결성·기밀성의 원칙 등 6가지 원칙이 강조됨.**

- 컨트롤러는 상기 원칙을 준수할 책임을 지며 이를 입증할 수 있어야 한다는 책임성의 원칙을 부담함(제5조).[8]
- GDPR은 처리의 적법성과 관련하여 동의의 기준을 높임(제7조).
  - 동의는 자유로운 의사에 의해 이루어져야 하며, 동의 획득 시 컨트롤러의 신원, 개인정보 처리의 목적, 언제든지 동의를 철회할 권리 등에 관해 구체적이고 명확한 정보가 제공되어야 함.
  - 동의는 정보주체의 진술 또는 적극적 행동을 통한 모호하지 않은 의사표시여야하며 간결하고 쉬운 언어를 사용하여야 함.

■ **[정보주체 권리 강화] 정보사회의 발전에 대응하여 EU 지침(Directive 95/46/EC)에는 없던 삭제권(잊혀질 권리), 처리제한권, 개인정보 이전권이 새롭게 도입되어 정보주체의 권리가 강화됨.**

- [삭제권 잊혀질 권리(right to be forgotten)라고도 하며, 정보주체는 본인에 대한 개인정보의 삭제를 컨트롤러에게 요구할 권리를 가지며, 요청에 따라 정당한 이유가 없는 한 삭제하여야 하고, 그 개인정보의 원래 이용자에게 정보주체가 삭제를 원하고 있음을 통지해야 함(제17조).
  - 개인정보가 원래의 수집·처리 목적에 더 이상 필요하지 않은 경우, 정보주체가 동의를 철회한 경우, 정보주체가 처리에 반대하는 경우, 개인정보가 불법적으로 처리된 경우, 법적 의무 준수를 위하여 삭제가 필요한 경우, 아동에게 정보사회서비스[9] 제공 관련 개인정보를 처리한 경우에 삭제권이 인정됨.
  - 표현 및 정보의 자유에 관한 권리 행사를 위한 경우 및 공익 등 GDPR에서 제시한 요건에 해당될 경우 삭제 요구를 거부할 수 있음.
- [처리제한권] 개인정보의 정확성, 개인정보 처리의 적법성 등에 대하여 다툼이 있거나 소송 수행 등을 위해 개인정보 보존의 필요가 있는 경우 정보주체가 임시로 컨트롤러에게 개인정보의 이용을 제한하거나 삭제를 보류하도록 요구할 수 있음(제18조).
  - 컨트롤러가 개인정보를 제3자에게 제공한 경우 제3자에게도 처리제한을 요구받은 사실을 통지하여야 하며, 정보주체의 요구에 의해 처리가 제한된 개인정보에 대해서 컨트롤러가 제한을 해제하기 위해서는 미리 정보주체에 그 사실을 알려야 함.

---

8) 컨트롤러(Controller): 개인정보 처리의 목적과 수단을 '결정'하는 주체를 의미하며, 그 결정은 컨트롤러 단독으로 하거나 제3자와 공동으로 할 수 있음. 자연인을 비롯하여 법인, 공공기관, 에이전시, 기타 단체 등이 컨트롤러가 될 수 있음.

9) 정보사회서비스(Information Society Service): 서비스를 제공받는 자의 개별적 요청에 따라 원격에서 전자적 수단을 통하여 통상 영리(remuneration) 목적으로 제공되는 서비스.

- [개인정보 이전권] 정보주체는 컨트롤러에게 제공한 자신의 개인정보를 제공받을 권리가 있으며, 다른 컨트롤러에게 자기정보의 이전을 요구할 권리가 있음(제20조).

○ 컨트롤러는 정보의 상호유용성(interoperability)을 보장할 수 있도록 개인정보를 구조적이며 보편적으로 사용되는 기계판독이 가능한 형태로 제공받을 권리가 있으며 그 정보를 다른 컨트롤러에게 제공할 것을 요구할 수도 있음.

○ 개인정보 이전권은 정보주체의 선택권 확대를 통해 대기업은 물론 중소기업의 개인정보 접근성을 제고해줌으로써 기업 간 공정한 경쟁환경 조성을 목적으로 함.

표 3. GDPR 정보주체 권리

정보주체 권리	조문	내용
정보를 고지받을 권리 (Right to be informed)	제13조 제14조	컨트롤러는 정보주체에게 개인정보 처리와 관련된 정보를 알려야 함. 정보는 명확하고 쉬운 언어로 무상으로 제공되어야 함.
열람권 (Right to access)	제15조	컨트롤러는 열람 요구에 따른 사본 무상제공 등 정보주체의 열람권을 보장하기 위해 필요한 조치를 취해야 함.
정정권 (Right to rectification)	제16조	정보주체는 부정확하거나 불완전한 개인정보에 대해 정정을 요구할 권리가 있음.
삭제권 (Right to erasure)	제17조	개인정보가 원래의 수집처리 목적에 더 이상 필요하지 않은 경우나 정보주체가 동의를 철회한 경우 등에서 삭제권을 보장하여야 함.
처리제한권 (Right to restriction of processing)	제18조	개인정보의 정확성에 이의가 있거나 불법적인 처리에 대하여 삭제 대신 처리제한을 선택하는 등 개인정보 처리제한 요구를 받은 경우, 특별한 경우를 제외하고는 컨트롤러는 개인정보를 처리할 수 없음.
개인정보 이전권 (Right to data portability)	제20조	정보주체는 개인정보를 여러 다른 서비스에 걸쳐 재사용할 수 있도록 자기정보의 이전을 요구할 수 있음.
반대권 (Right to object)	제21조	정보주체는 프로파일링 등 직접마케팅, 컨트롤러의 정당한 이익 또는 공익적 임무 수행 및 직무권한 행사에 근거한 처리, 과학적·역사적 연구 및 통계 목적 처리의 경우 본인과 관련한 개인정보의 처리에 대하여 반대할 권리를 가짐.
자동화된 의사결정(프로파일링[10])에 대한 권리 (Right related to automated decision making, including profiling)	제22조	프로파일링을 포함한 자동화된 의사결정은 계약이행을 위해 필요한 경우, EU나 회원국 법률에서 승인한 경우, 정보주체의 명시적인 동의를 획득한 경우에만 허용됨.

■ [정보의 목적 외 처리 허용] GDPR은 빅데이터 시대에 발맞추어 목적 외 처리에 대해 상당히 유연한 접근을 하고 있음(제6조 제4항).

- ① 목적 외 처리가 정보주체의 동의를 얻은 경우, ② 제23조 제1항상 목적[11]을 위한 경우, ③ EU 또는 회원국의 법에 근거한 경우 등임.

○ 양립가능성 판단 기준으로 i) 최초 수집 목적과 추가적 처리를 위한 목적 사이의 연관성, ii) 정보주체와 컨트롤러 관계를 고려하여 수집되는 전후 상황, iii) 민감정보 및 범죄기록 처리 여부 등 처리되는 개인정보 특성, iv) 정보주체에게 미칠 수 있는 결과, v) 적절한 안전장치(safeguards)로 암호처리 또는 가명처리 여부가 고려됨.

10) 프로파일링(profiling): 정보주체의 개인적인 측면(직장 내 업무성과, 경제 상황, 건강, 취향 등)을 분석 및 예측하기 위한 자동 처리.

11) GDPR 제23조 제1항에 규정된 목적으로는 국가안보, 국방, 공공안전, 범죄의 예방, 조사, 적발, 기소 또는 형사처분 집행(공공안전 확보 및 공공안전에 대한 위협의 예방을 포함), 그밖에 유럽연합 또는 회원국의 공익상 중요한 목적으로, 특히 EU 또는 회원국의 중요한 경제적·재정적 이익, 사법독립과 사법절차의 보호, 직업적 윤리의 위반에 대한 예방, 조사, 적발 및 기소, 상기 언급된 사항에 대한 공공기관의 감독 및 조사, 정보주체의 보호와 정보주체가 아닌 다른 사람의 권리와 자유, 민사청구의 집행이 있음.

○ 양립가능하다는 판단하에 정보주체의 동의나 별도의 법적 근거 없이 목적 외 처리가 가능함.

- GDPR은 개인정보의 목적 외 처리에 대해 원칙적으로는 금지하고 있으나 '제89조 제1항에 따른 공익을 위한 기록보존 목적, 과학적 또는 역사적 연구 목적, 또는 통계적 목적'은 원래의 수집 목적과 양립 가능한 것으로 간주된다고 규정함(제5조 제1항 b).

■ [컨트롤러와 프로세서의 책임 강화] GDPR은 컨트롤러와 프로세서의 책임을 강화함.

- 컨트롤러는 적절한 문서화 의무(제30조), 개인정보보호 최적화 설계 및 기본설정 원칙을 충족하는 내부 정책과 조치를 채택할 의무(제25조), 고위험 개인정보 처리에 대한 개인정보 영향평가 수행 의무(제35조), 개인정보 보호책임관(DPO) 지정 의무(제37조), 개인정보 침해 발생 시 통지 의무(제33조, 제34조), 개인정보 국외전송 기준 준수(제5장), 국가 감독기구협조의무(제31조) 등을 준수하여야 함.
- 프로세서에 대해서도 적절한 문서화 의무(제30조), 적절한 보안기준 적용 및 개인정보 영향평가 수행(제32조), 개인정보 국외전송 기준 준수(제5장), 국가 감독기구협조의무(제31조) 등이 부과됨.[12)]

■ [적절한 문서화 의무] 컨트롤러와 프로세서는 GDPR 의무 준수를 입증하기 위하여 본인의 책임하에 개인정보 처리활동의 기록을 문서(전자문서 포함)로 유지해야 함(제30조).

- 영세 또는 중소기업들의 상황을 고려해 종업원 수 250명 이상의 기업에 대해서만 개인정보 처리활동에 관한 기록을 의무적으로 문서화하도록 규정함.
- 그러나 종업원 수 250명 이하라도 ① 정보주체의 권리와 자유에 위험을 초래할 가능성이 있는 개인정보, ② 민감정보, ③ 범죄경력 및 범죄행위와 관련한 개인정보 처리 시에는 반드시 처리활동 기록이 필요함.
- 대상 기업은 ① 컨트롤러의 이름 및 연락처, ② 처리의 목적, ③ 정보주체의 유형 및 개인정보의 범주, ④ 개인정보 수령인의 범주, ⑤ (적용 시) 제3국으로 개인정보가 이전되는 경우에 국외이전 방식과 보호조치, ⑥ (가능할 경우) 보유기간, ⑦ (가능할 경우) 기술적·관리적 보호조치를 문서화해야 함.

■ [개인정보보호 최적화 설계 및 기본설정] 컨트롤러는 개인정보보호를 위해 개인정보보호 최적화 설계 및 기본설정(Data protection by design and by default) 원칙을 충족하여야 함(제25조).

- [개인정보보호 최적화 설계] 컨트롤러는 개인정보 처리로 인해 개인의 권리와 자유에 영향을 미치는 다양한 발생 가능한 위험과 그 위험의 심각성을 고려하여 적절한 기술적·관리적 조치를 실시해야 함.

○ 이러한 조치에는 개인정보 처리의 최소화, 처리에 필요한 보호조치(safeguards), 가명처리[13)] 등이 포함됨.

- [개인정보보호 기본설정] 개인정보 처리가 되는 제품, 서비스, 애플리케이션의 기본설정은 개인정보 처리 목적을 위한 최소한의 범위 내에서 개인정보가 활용되도록 이루어져야 함.

12) 프로세서(Processor): 컨트롤러를 대신하여 개인정보를 '처리'하는 자연인, 법인, 공공기관, 에이전시, 기타 단체를 의미하며 컨트롤러의 지시에 따라 개인정보를 처리함.

13) 가명처리(pseudonymisation): 개인정보를 수정·가공하여 추가적인 정보를 사용하지 않고는 더 이상 원래의 개인정보를 알아볼 수 없는 상태로 만드는 것을 의미함. 이와 같은 추가적인 정보는 분리하여 보관하고 해당 정보를 통해 자연인을 식별하지 않도록 기술적·관리적 조치를 취해야 함.

■ [고위험 개인정보 처리에 대한 개인정보 영향평가] 컨트롤러는 새로운 기술을 사용하고, 그 정보처리 유형이 개인의 권리와 자유에 고위험을 초래할 가능성이 있는 경우, 개인정보를 처리하기 이전에 개인정보보호 영향평가를 수행해야 함(제35조).

- 특히 개인정보보호 영향평가는 ① 프로파일링 등 자동화된 처리에 근거하여 자연인에 대한 체계적이고 광범위한 평가를 하는 경우로서, 해당 평가에 기반한 결정이 정보주체에게 법적 효력이 있거나 이와 유사하게 중대한 영향을 미치는 경우, ② 민감정보 또는 유죄판결/형사범죄에 대한 대규모 처리를 하는 경우, ③ 공개적으로 접근가능한 장소에 대한 대규모의 체계적인 모니터링을 하는 경우 요구됨.

■ [DPO 지정] ① 공공기관이거나, ② 컨트롤러 또는 프로세서의 핵심활동이 정보주체에 대한 대규모의 정기적이고 체계적인 모니터링 또는 민감정보나 범죄경력 및 범죄행위에 대한 대규모 처리인 경우 개인정보보호책임관(DPO: Data protection officer)을 지정하여야 함(제37조).

- DPO는 ① 컨트롤러, 프로세서 및 임직원에게 GDPR 등 관련 법규 준수 의무에 대한 고지 및 자문, ② 기업의 GDPR 및 다른 정보보호 법규 이행상황 모니터링, ③ 컨트롤러 또는 프로세서에게 정보 제공 및 권고사항 제시, ④ 개인정보 영향평가에 대한 자문 및 평가 이행을 감시하는 역할을 함(제39조).
- DPO에게 요구되는 전문지식의 수준은 DPO가 수행하는 처리작업과 보호수준에 따라 결정되며, DPO는 GDPR을 준수하지 않는 데에 대해 개인적인 책임을 지지는 않음.

■ [개인정보 침해 발생 시 조치사항] 컨트롤러는 개인정보 유출 발생 시 그 사실을 알게 된 때로부터 72시간 내에 감독당국에 보고해야 하며, 프로세서는 개인정보 유출사실을 알게 된 때에 컨트롤러에게 그 사실을 부당한 지체 없이 알려야 함(제33조).

- 개인의 권리와 자유에 위험을 야기할 가능성이 있는 침해가 발생한 경우(예: 차별행위, 평판 훼손, 재정적 손실, 비밀 누설 등) 인지 후 지체 없이 가능한 72시간 이내 감독당국에 보고(제33조)
- 개인의 권리와 자유에 고위험을 야기할 가능성이 있는 경우 인지 후 부당한 지체 없이 정보주체에게 직접 통지해야 함(제34조).

■ [개인정보의 역외이전] GDPR은 EU 역내에서는 정보의 자유로운 이동을 보장하고 있는 반면, EU 역외로 개인정보를 이전하는 경우 ① 제3국이 적정성 평가 승인을 획득한 경우이거나, ② 개인정보를 이전하려는 기업이 적절한 보호조치를 갖춘 경우로 제한함.

- [적정성 결정 승인에 따른 이전] GDPR은 개인정보 국외이전의 대표적인 허용 사유로서 적정성 결정(adequacy decision)을 승인받은 EU 역외국으로의 이전을 들고 있음(제45조).
  - ◦ EU 집행위원회는 ① 제3국, ② 제3국의 영토 또는 하나 이상의 특정 부분, ③ 국제기구가 적정한 수준의 보호(adequate level of protection)를 보장한다고 판단한 경우, 제3국국제기구로 개인정보를 이전하는 것이 가능함.
  - ◦ EU 지침과 달리 사후 감시의무를 도입하여 적정성 요건 결여 시 철회가 가능함.

○ 2018년 5월 기준으로 EU로부터 적정성 평가를 승인받은 국가는 모두 12국으로 안도라, 아르헨티나, 캐나다(상업기관에 한정하여 부분 승인), 페로 제도(Faroe Islands), 건지(Guernsey), 맨 섬(Isle of Man), 이스라엘, 저지, 뉴질랜드, 스위스, 우루과이, 미국(Privacy Shield에 제한)이며, 한국과 일본은 적정성 평가를 진행 중에 있음.[14]

- [적절한 보호조치에 따른 이전] 적정성 결정이 없더라도 컨트롤러나 프로세서가 적절한 보호조치(appropriate safeguards)를 제공할 경우 역외이전이 허용됨(제46조).

○ 공공당국 또는 기관 사이의 법적 구속력이 있고 집행가능한 문서, 구속력 있는 기업규칙(BCR: Binding Corporate Rules), EU 집행위원회가 채택한 표준개인정보보호조항, 감독당국이 채택하고 유럽위원회가 승인한 표준개인정보보호조항, 승인된 행동 규약(Approved Code of Conduct), 승인된 인증 메커니즘(Approved Certification Mechanism) 등에 대해 역외이전 허용

- 1995년 EU 지침은 감독당국이 채택하는 표준조항을 적절한 안전조치로 규정하지 않았으며, 행동규약을 권장하지만 EU 역외이전의 근거로 명시적으로 허용하지 않고, 인증도 역외이전의 근거로 규정하지 않았으나, GDPR에서는 적절한 안전장치로 포함함.

- [기타 허용사유] 다음의 경우에도 예외적으로 제3국으로의 개인정보 이전을 허용함.

○ 정보주체가 적정성 결정 및 적절한 보호조치가 없음으로 인해 발생할 수 있는 위험을 고지 받은 후 명시적으로 동의한 경우, 정보주체와의 계약 이행을 위해 정보이전을 해야 하는 경우, 중요한 공익상의 이유로 정보이전이 필요한 경우, 법적 권리의 확립, 행사, 수호를 위해 정보 이전이 필요한 경우, 정보주체가 물리적 또는 법률적으로 동의를 할 수 없는 경우에 정보주체 또는 타인의 생명과 관련한 주요 이익을 보호하기 위해 정보이전이 필요한 경우 등에도 예외적으로 이전을 인정함(제49조).

■ **[감독기관의 강화] EU 지침에서는 감독기관의 권한으로 조사권, 실효적인 중재권과 법적 쟁송참가권만을 규정했으나, GDPR은 컨트롤러에 대한 규칙위반 시정명령권 등 강력하고 폭넓은 감독권한을 부여함(제58조).**

- [One-Stop Shop] 복수의 EU 회원국에 주재하는 컨트롤러를 위하여 One-Stop Shop 개념을 도입하여 주 사업장의 감독기관을 선임감독기관(lead supervisory authority)으로 지정하고 EU 내 회원국에 공통적으로 관련된 개인정보 이슈에 대해 주관하도록 함(제56조).

○ 필요시 총괄 감독기관은 회원국의 감독기관과 협업하며, 단일국가에만 해당되는 사안의 경우 해당 국가 감독기관이 민원이나 위반을 처리할 권한을 가짐.

- EU 역내에서 개인정보보호에 관한 임무를 통일적이고 일관성 있게 수행하기 위하여 각 회원국의 감독기관의 수장으로 구성된 유럽정보보호이사회(European data protection board)를 설치함(제68조-제76조).

■ **[실효적 확보수단의 강화] EU 감독당국은 GDPR의 의무 위반에 따른 벌칙에 관해 법규를 제정해야 하며, 행정적 제재와 관련하여 엄중한 과징금을 부과할 수 있도록 규정함.**

---

14) EU-미국 프라이버시실드(EU-US Privacy Shield framework)는 상업적으로 깊은 유대관계를 맺고 있는 양 지역 간 정보의 이동을 보호하기 위한 조치로서, 미국 기업은 강력한 정보보호 및 안전규정에 따라 개인정보를 처리하는 조건으로 EU에 위치한 미국기업이 수집한 개인정보를 미국 본사가 받을 수 있음. 프라이버시쉴드에 참여한 기업은 ① 개인정보 유형, ② 개인정보 처리 이유, ③ 다른 기업으로의 개인정보 이전 여부 및 이유, ④ 정보주체자의 개인정보 접근권한 여부, ⑤ 개인정보 사용 관련 불만제기 방법, ⑥ 프라이버시실드 관련 미국 내 관할 공공기관 등에 관한 정보를 제공함(https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en, 검색일: 2018. 5. 6).

- 과징금은 효과적이고, 비례적이며 억지력이 있도록 하여야 하며 각 감독당국은 다음을 고려함.

○ 각 개별사건에서 과징금의 부과 여부를 결정하고 과징금 액수를 결정할 때에는 관련 개인정보 처리의 성격, 범위 또는 목적을 고려한 위반의 성격, 중대성 및 기간, 손해의 정도, 고의과실, 컨트롤러와 프로세서가 취한 조치 등을 고려하여야 함(제83조).

○ GDPR에서는 일반 위반의 경우 1천만 유로까지 과징금 또는 사업체인 경우 직전 회계연도의 전 세계 매출액 2% 이하의 과징금 중 높은 금액을, 심각한 위반의 경우 2천만 유로까지 과징금 또는 직전 회계연도의 전 세계 매출액 4% 이하의 과징금 중 높은 금액을 과징금으로 부과할 수 있음.

표 4. EU GDPR 위반에 따른 과징금

과징금 규모	위반 내용
전 세계 연간 매출액 2% 까지 또는 1천만 유로까지 과징금 중 높은 금액 부과 (4항)	일반 위반 - 컨트롤러 및 프로세서 의무 위반(제8조, 제11조, 제25조-제39조, 제42조, 제43조) - 인증기관의 의무 위반 (제42조, 제43조) - 감시기관의 의무 위반(제41조 제4항)
전 세계 연간 매출액 4% 까지 또는 2천만 유로까지 과징금 중 높은 금액 부과 (5항)	심각한 위반 - 개인정보처리 6대 원칙 위반(제5조) - 개인정보 처리 적법성 요건 준수 위반(제6조) - 동의 여부 또는 동의의 유효성 입증 실패(제7조) - 민감정보 처리에 정보주체 명시적 동의 부재 등 조건 충족 실패(제9조) - 정보주체의 권리보장 의무 위반(제12조-제22조) - 역외이전(제44조-제49조) - 제9장에 따라 채택된 EU 회원국 법률 의무 위반 - 감독기구가 내린 명령 또는 정보 처리의 제한 불복(제58조 제2항) - 개인정보이동 중지 미준수 및 열람기회 제공 의무 위반(제58조 제1항)

3. EU GDPR의 파급효과

■ EU 데이터 시장 및 데이터 경제에 대한 전반적인 시장가치가 지속적인 증가세에 있는 만큼 EU GDPR이 미칠 영향을 무시할 수 없음.

- EU의 데이터 시장 가치는 2013년 474억 유로에서 2017년 650억 유로로 꾸준히 증가하고 있고, 2025년까지 961억 유로~1,464억 유로로 증가할 것으로 보임.[15]

○ 2017년 기준, EU 회원국 중 영국의 데이터 시장 가치는 146억 유로로 가장 크며, 다음으로 독일(143억 유로), 프랑스(81억 유로), 이탈리아(50억 유로) 순임(그림 3 참고).

○ 산업별 데이터 시장 가치는 제조업 분야가 140억 유로로 가장 크며, 다음으로 금융서비스(130억 유로), 전문서비스(91억 유로), 도소매(70억 유로) 순임(그림 4 참고).

- 한편 EU의 데이터 경제 가치는 2017년 기준 3,356억 유로에 이르며, 2025년까지 4,700억 유로~6,692억 유로로 증가할 것으로 전망됨.

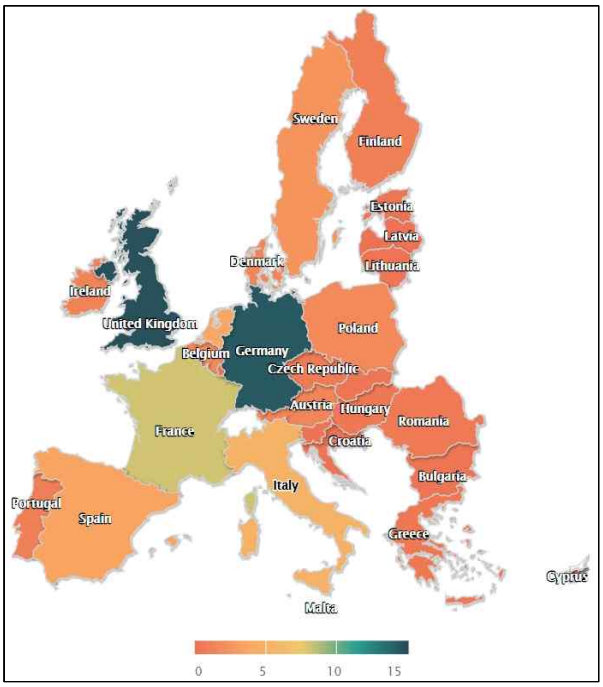
○ 데이터 경제는 데이터의 생성, 수집, 저장, 처리, 분배, 전달을 모두 포괄하는 개념으로, EU는 2017년 발표한 유럽

15) 데이터 시장(Data Market)은 로 데이터(Raw data)의 가공결과 생산된 디지털 데이터가 재화나 서비스로 교환되는 곳을 의미하며, 시장가치는 디지털 데이터의 총수요가치를 의미함.

데이터 경제육성정책을 통해 데이터에 대한 자유로운 접근과 분석역량을 강화함으로써 새로운 비즈니스 모델을 개발한다는 목표를 설정함.[16]

그림 3. 2017년 EU 회원국별 데이터 시장 가치

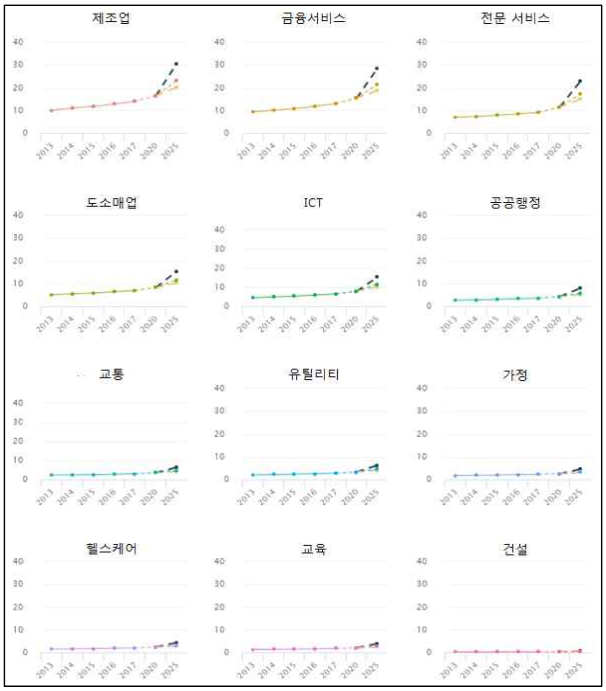
(단위: 십억 유로)



자료: European Data Market Monitoring Tool(2018).

그림 4. EU 산업별 데이터 시장 가치

(단위: 십억 유로)



자료: European Data Market Monitoring Tool(2018).

■ EU GDPR의 경제적 효과를 긍정적으로 분석하는 연구로는 EU 집행위와 Buchholtz *et al.*(2014)이 대표적임.

- EU 집행위는 EU GDPR이 다음과 같은 측면에서 디지털 단일시장의 심화에 긍정적으로 기여할 것으로 평가함.[17]

○ 기존 개인정보보호제도하에서 새롭게 EU GDPR을 적용하는 데 드는 비용은 1억 3천만 유로인 반면, EU 단일의 개인정보보호제도 도입으로 인한 경제적 편익은 23억 유로로 추산함.

○ 기업들은 개인정보와 관련하여 EU 28개국이 아닌 하나의 감독당국과 협의를 해도 무방하기 때문에 더 단순하고, 비용효율적인 기업 비즈니스가 가능해짐.

○ 설립지와 상관없이 모든 기업들을 대상으로 단일 법규정이 적용되기 때문에 EU 기업과 비EU 기업 간 공정경쟁이 가능하다는 점도 강조

○ 새로운 개인정보보호법하에서 기업들의 관련 기술혁신이 장려될 것으로 예상됨.

- Buchholtz *et al.*(2014)은 개인정보보호조치 강화와 기업의 사업기회 증대가 균형을 이룰 경우 EU의 GDP가 2020년까지 1.9% 증가할 수 있다고 전망함.[18]

16) https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy(검색일: 2018. 5. 7).
17) http://ec.europa.eu/justice/smedataprotect/index_en.htm(검색일: 2018. 5. 9).
18) Sonia Buchholtz *et al.*(2014), "Big and Open Data in the Europe – A Growth engine or a missed opportunity?" Report Commissioned by demosEUROPA 2014.

■ 반면 EU GDPR이 기업들에게 편익보다는 새로운 비용과 부담을 유발함으로써 경제 전반에 부정적인 효과를 초래할 것으로 전망하는 연구결과들도 있음.

- 영국 법무부는 GDPR에 따른 회원국별 상이한 법제도 조화의 이익보다 규제 강화에 따른 비용부담이 클 것으로 평가함.[19]
  - ○ 영국 IT 기업들의 경우 GDPR에 대응하기 위한 순비용이 1차 연도에 2억 5천만 파운드로 추산됨.
- Pyykkö(2012)는 GDPR이 모든 산업 부문에 보호조치 강화를 요구함으로써 금융서비스 발전을 저해하고, 이에 따라 신용공급의 위축과 EU의 경제성장 잠식이 우려된다고 발표함.[20]
- Christensen *et al.*(2013)은 GDPR 준수를 위해 연간 EU 기업들이 지불해야 하는 IT 비용은 20% 증가할 것으로 전망함.[21]
  - ○ EU 역내 중소기업은 GDPR 적응 비용으로 연간 3,000~7,200유로가 필요하며, 이는 중소기업 연간 예산의 16~40%에 해당됨.
  - ○ 특히 DPO를 선임하는 비용은 2만 5천~5만 유로로 중소기업에 적지 않은 비용부담이 될 것으로 예상됨.
- 가장 최근에 발표된 London Economics(2017)는 GDPR 시행은 EU에 580억 파운드의 경제손실과 130만 일자리 감소를 초래할 것으로 전망함.[22]

■ EU GDPR은 단기적으로는 새로운 인프라 구축 및 조직개편, 혁신적인 중소벤처 스타트업 출범의 어려움 등 사회경제적 비용을 유발할 수 있으나, 중장기적으로 개인정보보호 강화에 따른 소비자 신뢰 증가와 국경 간 정보이동의 자유로움 증대라는 측면에서 사회경제적 편익이 더 클 수 있을 것으로 판단됨.

- GDPR 대응과정에서 다양한 기업들이 비즈니스 모델을 수정하거나 조직을 개편할 것으로 예상되며, 그 대응의 수준에 따라 해당 기업 및 경제에 미칠 영향도 매우 상이할 것으로 판단됨.
  - ○ GDPR이 적용대상을 특정하지 않고, EU 역내 거주자에게 재화와 용역을 제공하는 모든 기업을 대상으로 하고 있기 때문임.
  - ○ 기업의 경우 GDPR이 요구하는 개인정보보호 규정을 준수하기 위해 추가 재원을 투입하거나, 아예 유럽에서의 사업을 중단하는 선택지가 있기 때문에 기업의 선택에 따른 효과 추정에 어려움이 존재함.

4. 평가 및 대응방안

■ EU 회원국별 서로 다른 개인정보보호 제도와 법 규정으로 인해 EU 단일시장 심화가 지체되고 있다는 판단에 따라 제안된 EU GDPR은 디지털 시대에 데이터 보호에 대한 가장 포괄적이며 미래지향적인 입법으로 향후 개인정보보호에

19) UK Ministry of Justice(2012), "Proposal for a EU Data Protection Regulation – Impact Assessment(IA)."
20) Elina Pyykkö(2012), "Data Protection at the cost of economic growth?" *ECRI Commentary No. 11/Nov. 2012.*
21) L. Christensen *et al.*(2013), "The Impact of the Data Protection Regulation in the EU," *International Think-tank on Innovation and Competition INTERTIC Feb 2013.*
22) London Economics(2017), *Analysis of the potential economic impact of GDPR: Implications of the ICO's Draft Guidelines on consent.*

관한 글로벌 표준 정립에 영향을 미칠 것으로 판단됨.

- 개인정보보호 수준 강화로 신뢰를 높이며, 익명정보 대상 제외, 다양한 방식으로 국외 이전 허용 등 자유로운 정보이동 촉진을 위한 장치를 마련하는 EU GDPR의 주요 내용은 EU 이외의 국가 및 기업에 개인정보 활용에 대한 관행의 변화를 촉구할 것으로 예상됨.

○ 다국적 기업들의 경우 개인정보를 수집하는 과정에서 개인정보의 사용내역을 제대로 명시하지 못했다는 비판을 받고 있음.

○ GDPR은 개인정보에 대한 정보주체자의 명시적 동의를 요구하면서, 기업들은 개인정보 수집 시 사용목적에 따라 별도로 정보주체자의 동의를 받아야 하는 'Opt-In' 방식을 분명히 함.

○ 주요 언론들은 GDPR이 유럽의 개인정보보호 기준을 전 세계에 수출하고 있다고 평가하면서, 이를 두고 '브뤼셀 효과'라고 명명하기도 함.[23]

- 미국은 EU GDPR을 자국 기업을 대상으로 하는 보호무역조치라고 강하게 비판하는 반면, EU는 디지털 경제 시대 개인정보보호를 강화하고 기업 비즈니스를 장려하기 위한 조치임을 강조함.

○ Hofheinz and Mandel(2014)은 GDPR의 개인정보보호 수준이 일반적인 소비자 정보를 보호하는 수준을 넘어서는 과도한 규제이며, EU 시장에서 경쟁력을 확보한 미국기업에 상대적으로 큰 부담을 초래할 것으로 평가함.[24]

○ EU 집행위는 GDPR이 국경 간 정보의 자유로운 이동 및 범대서양 서비스 교역을 저해하려는 목적이 아니며, 오히려 EU와 미국 간 디지털 서비스 규제 불일치를 개선하는 데 도움이 될 것으로 평가함.

○ 또한 EU 집행위는 GDPR의, EU 역내외 모든 기업을 대상으로 하는 차별 없는 규제적용은 보호무역조치로 볼 수 없음을 강조함.

- EU GDPR은 1995년 EU 지침의 개인정보보호 강화라는 목적을 승계하고 있다는 점에서 기존에 없던 혁신이 아닌 진화로 평가되며, 향후 개인정보에 관한 새로운 글로벌 표준을 정립하는 데 영향을 미칠 것으로 판단됨.

○ EU 역내에 재화와 용역을 제공하는 모든 기업들은 GDPR이 요구하는 법적 의무사항을 기업 비즈니스에 반영하고 이에 적응한다면 EU GDPR이 글로벌 표준으로 작용할 가능성도 함께 제고될 것으로 전망됨.

○ OECD와 EU가 글로벌 개인정보보호에서 기준을 제공하는 주요 행위자임을 고려할 때, EU GDPR은 향후 개별국이 新개인정보보호법을 입법하는 과정에서 핵심 규제내용으로 반영될 가능성이 클 것으로 판단됨.

○ 한편 GDPR 99개 조문 중 약 69개 조문이 EU 회원국에게 일종의 자유재량을 위임하는 형식의 오프닝조항으로 규정되어 있는바, 향후 각국의 개인정보보호법 입법과정에 대한 모니터링이 필요함.

- 한편 개도국들이 EU GDPR의 높은 개인정보보호 수준을 충족하는 데 어려움이 예상되며, 결과적으로 글로벌 정보공유체인(Data-Sharing Chain)에서 개도국의 정보보호의 취약성을 개선하기 위한 교육, 법제도 등에 투자가 요구됨.[25]

○ 개도국의 열악한 정보보호 기술수준과 미흡한 법제도는 개인정보보호에 많은 행정비용을 유발할 수 있음.

---

23) https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation/(검색일: 2018. 5. 7); https://www.ft.com/content/777a1d34-ceb4-11e7-b781-794ce08b24dc(검색일: 2018. 5. 7).

24) Paul Hofheinz and Michael Mandel(2014), "Bridging the Data Gap: How Digital Innovation Can Drive Growth and Create Jobs," *Progressive Policy Institute Issue 15/2014.* The Lisbon Council.

25) Tiffany Curtiss(2016), "Privacy Harmonization and the Developing World: The Impact of the EU's General Data Protection Regulation on Developing Economies," *Washington Journal of Law, Technology &Arts,* Vol.12, Issue 1.

■ [한국의 개인정보보호와 활용 균형을 위한 법제 개선] 한국 개인정보보호 법제의 개인정보보호와 활용의 균형을 맞추기 위한 개선 노력이 필요함.

- 한국의 개인정보보호법은 개인의 자유와 권리를 보호하고 나아가 개인의 존엄과 가치를 구현함을 목적으로 하고 있어 개인정보의 자유로운 이동 등 활용 측면은 고려하지 않고 있음.[26]
  - ○ EU GDPR을 비롯하여 OECD 가이드라인 및 APEC Privacy Framework 등에서는 개인정보보호뿐만 아니라 개인정보의 이동과 같은 활용 측면이 법률적 취지로 고려됨.
  - ○ GDPR에서는 영리목적이라 하더라도 가명처리·암호화처리 등의 안전조치를 통한 목적 외 처리를 허용하고 있어, 개인정보 분석을 통한 새로운 서비스 산업 활성화를 촉진함. 반면 한국은 개인정보 활용 및 공유에 엄격한 제한을 부과함.[27]
- 한국 외교부는 5월 10일 관계부처 합동 보도자료를 통해 EU GDPR에 대한 정부 합동체계를 구축하여 기업들을 지원할 계획임을 발표함.[28]

■ [적정성 결정 승인 노력] EU 역내의 개인정보를 역외 국가로 이전하는 경우 EU 당국의 승인이 필수적이나, 국가 차원에서 EU의 '적정성 결정(adequacy decisions)'을 승인받은 경우는 별도의 기업의 개인정보 이전 계약이 요구되지 않는바, 한국정부는 EU 집행위원회가 빨리 적정성 결정을 승인하도록 적극적으로 협상할 필요가 있음.

- 적정성 결정은 제3국이 EU가 요구하는 개인정보보호 수준을 갖추고 있는지 평가하는 것으로, 한국정부도 개인정보 해외이전에 관한 적정성 결정을 최우선 사안으로 인지하고 진행하고 있음.
  - ○ 적정성 결정 승인은 EU 집행위의 제안, 유럽개인정보보호이사회 의견 검토, EU 회원국 대표들의 승인, EU 집행위의 결정 순으로 진행됨.
- 적정성 평가는 신청 시점 기준으로 결정시한이 별도로 정해져 있지 않기 때문에 EU가 적정성 평가 일정을 편의적으로 조정할 수 있음. 이에 EU의 적정성 평가 승인을 기다리고 있는 한국정부는 EU의 적정성 평가 승인을 얻어내기 위해 정부 차원의 법적·제도적 기반을 마련하고 및 EU에 적극적으로 이와 같은 정보를 제공할 필요가 있음.[29]
  - ○ 우리나라는 아직 적정성 결정을 획득하지 못한 관계로 EU 내 정보주체의 개인정보를 국내로 이전하기 위해서는 구속력 있는 기업규칙(BCR) 또는 표준 개인정보보호 조항 등의 적절한 보호조치 요건을 갖추거나 정보주체의 명시적 동의를 받거나 중요한 공익상의 이유가 인정되는 등의 허용사유가 있어야 함.
  - ○ 적정성 평가 승인을 통해 한국 내 중소기업들이 별도로 GDPR이 요구하는 개인정보보호를 위해 필요한 비용을 절감해줄 수 있다는 점에서 의미가 있음.

---

26) 개인정보보호법 제1조(목적) 이 법은 개인정보의 처리 및 보호에 관한 사항을 정함으로써 개인의 자유와 권리를 보호하고, 나아가 개인의 존엄과 가치를 구현함을 목적으로 한다.

27) 한국 개인정보보호법 제18조 제2항 제4호에 따르면 '통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우'는 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있음. '통계 작성 및 학술연구 등의 목적'을 비영리에 한정하는 견해가 다수이며, 특정 개인을 알아볼 수 없는 형태를 가명처리가 아닌 익명화로 이해하는 견해도 적지 않은바, 조문의 명확성을 높여 법적 불확실성을 없애기 위한 작업이 필요함.

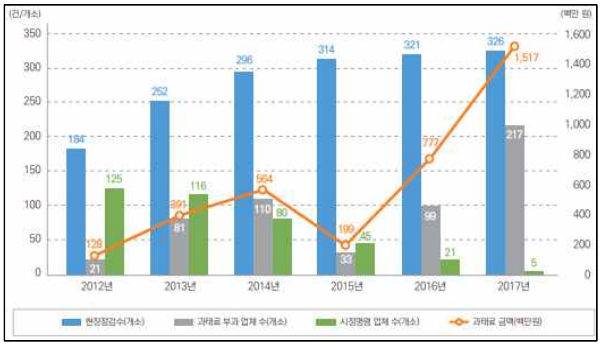
28) 외교부(2018. 5. 10), 「EU의 개인정보보호 강화 대비, 기업준비사항 안내에 정부부처 한마음- 외교부, 국무조정실, 방통위, 산업부, 중기부, 행안부 등 관계부처 협력」.

29) European Commission(2017), "Press statement by Commissioner Věra Jourová, Mr. Lee Hyo-seong, Chairman of the Korea Communication Commission and Mr. Jeong Hyun-cheol, Vice President of the Korea Internet & Security Agency"; EU는 한국뿐만 아니라 일본에 대해서도 적정성을 평가하고 있음.

■ [개인정보보호에 관한 기업 인식 및 대응 지원] 한국정부는 기업들의 개인정보보호 인식 제고를 통해 EU GDPR에 적응할 수 있도록 하는 지원책을 수립하고 이행해야 함.

- 2018년 4월 행정안전부가 발표한 자료에 따르면, 국내 개인정보보호 강화노력에 따라 많은 개선이 이루어지고 있으나, 여전히 개선의 여지가 큰 것으로 나타남.30)
  - ○ 현장점검에 따른 과태료 부과 및 시정명령이 최근 3년간 급증했으며, 개인정보 유출 신고 건수도 2017년 다시 증가함.
  - ○ 정부는 민간사업자 및 공공기관을 대상으로 하는 개인정보보호 관련 현장점검을 강화하는 것은 물론 평상시 사업을 추진하는 과정에서 수집한 개인정보를 보호할 수 있도록 기업가 및 시민들의 인식제고에 노력해야 함.
- 정부 및 감독기관을 중심으로 EU GDPR 관련 세미나 및 설명회를 개최하고, 기업의 법률적 자문수요 조사를 통한 지원책 마련이 효과적일 것으로 판단됨.31)

그림 5. 2012~17년 현장점검 및 행정처분



자료: 행정안전부(2018).

그림 6. 개인정보 유출 신고 건수 및 유출 건수

자료: 행정안전부(2018).

■ [기업의 사업전략 조정 및 조직 개편] EU 역내에 거주하는 사람들을 대상으로 재화와 용역을 제공하는 한국기업들은 기업 차원의 대응전략 수립이 요구되며, 동시에 EU GDPR 대응을 통해 소비자 신뢰를 제고하고 합법적·효과적으로 정보를 활용하는 기회로 삼아야 함.

- 기업들은 개인정보에 관해 지금까지와 다른 정책대응과 보호수준을 요구받고 있으며, 기업별로 대응해야 하는 수준 또한 상이하기 때문에 기업의 상황에 맞는 맞춤형 접근과 전략을 수립하는 것이 중요함.
  - ○ ① 개인정보 처리 최소화, ② 보관기간 제한의 원칙, ③ 무결성·기밀성의 원칙, ④ 목적 제한의 원칙, ⑤ 적법성·공정성·투명성의 원칙, ⑥ 정확성의 원칙 등 개인정보 처리 6대 원칙을 바탕으로 전략을 수립하는 것이 유용할 것으로 판단됨.32)
- EU GDPR의 적용을 받는 기업들은 기업책임성 강화 및 규정 준수를 위해 대응전략이 요구되며, 다음과 같은 단계별 접근법을 고려할 필요가 있음.33)

① 책임자 지정: 기업 내부에서 개인정보 관련 거버넌스 책임자(DPO)를 지정하고, 책임자를 중심으로 조직을 구성할

30) 행정안전부(2018), 『2013~2017 개인정보 실태 점검 및 행정 처분 사례집』.
31) EU 집행위원회도 GDPR에 대한 기업들의 이해제고를 위해 주요 이슈별 가이드라인을 발표하고 있음[부록 표 2 참고].
32) 한국인터넷진흥원(2017), 『우리 기업을 위한 유럽 일반 개인정보보호법(GDPR) 1차 가이드라인』, p. 9.
33) https://www.cnil.fr/fr/principes-cles/rgpd-se-preparer-en-6-etapes(검색일: 2018. 5. 10).

수 있도록 해야 함.

② 개인정보 처리와 관련한 흐름도 작성: 명확하게 개인정보 구축, 처리, 이동, 결정을 확인할 수 있도록 기업 내 흐름도를 작성하는 것이 필요함.

③ 우선순위 선정: 현재 및 미래의 개인정보 준수와 관련한 행동계획을 우선순위에 따라 작성함.

④ 리스크 관리: 개인정보를 처리하는 과정에서 발생할 수 있는 리스크를 관리하기 위해 개인정보보호 영향평가(DPIA: Data Protection Impact Assessment)를 시행함.

⑤ 내부 정책결정 과정 수립: 개인정보보호와 관련하여 기업 내 모든 사업영역에서 고려될 수 있도록 하는 것이 중요하며, 예상가능한 모든 시나리오별 정책대응을 위한 내부절차 이행

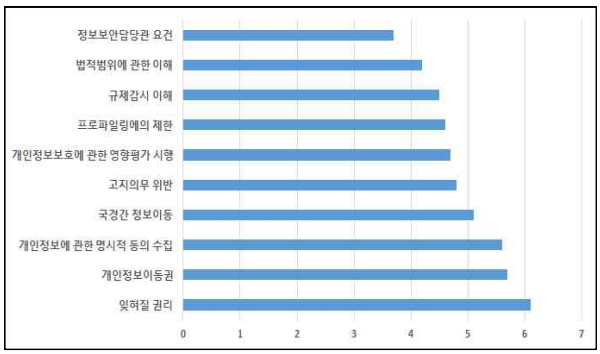
⑥ 개인정보 관련 모든 단계별 문서화: 개인정보보호와 관련하여 각 단계별로 보고서 작성을 의무화

- EU GDPR에서 새롭게 도입된 규정 중 기업별로 요건에 대한 준비상황을 점검하고, 준비요건별로 우선순위를 정해 GDPR에 준비해야 함.

○ 유럽의 기업들을 대상으로 한 설문조사에서 GDPR 항목 중 ① 잊혀질 권리(삭제권), ② 개인정보이전권, ③ 개인정보에 관한 명시적 동의, ④ 국경 간 정보이동에 대한 준수가 상대적으로 어렵다는 의견이 제시됨(그림 7 참고).[34]

○ 기업들은 사업 추진 시 필수적인 정보를 확정한 후, EU GDPR이 요구하는 규정을 준수하기 위한 기업 내 우선순위 및 추진계획을 수립하는 것이 중요함.

그림 7. GDPR 규정 준수의 어려움 정도



주: 1) 2016년 기준 기업설문조사.
2) 준수의 어려움 정도는 0~10으로 표시되며, 0 = 전혀 어렵지 않음, 10 = 매우 어려움을 의미.
자료: PWC(2017) 자료 활용하여 저자 작성.

- 4차 산업혁명에서 정보의 가치가 중요해짐과 동시에 정보에 대한 강력한 보안 및 보호는 기업의 경쟁력을 나타내는 지표로 사용될 수 있는바, 기업들은 EU GDPR 대응과정을 소비자의 신뢰를 제고하고 사업경쟁력을 강화하는 기회로 활용할 수 있도록 인식전환이 요구됨. KIEP

34) EU GDPR의 입법 과정에서 미국기업들은 개인정보에 관한 명시적 동의가 기업에 많은 부담으로 작용한다는 판단에 따라, 이를 수정하도록 EU 집행위를 대상으로 전방위 로비활동을 벌이기도 했음.

부록 표 1. GDPR 개정안 일지

발표일	내용
2009년 6월	EU 집행위, 새로운 기술 및 글로벌화에 대응하여 개인정보보호의 위험요인에 관해 조사
2010년 11월	EU 집행위, 유럽의회와 EU 이사회에 개인정보보호를 위한 법제도 개정을 제안하는 커뮤니케이션 보고
2012년 1월	EU 집행위, 개인정보보호 개혁을 위한 개정안 초안 발표
2014년 3월	유럽의회, 법안에 대한 투표 및 승인
2014년 5월~2015년 6월	EU 이사회, GDPR 초안에 합의
2015년 12월	EU 집행위, 유럽의회 및 EU 이사회, GDPR 최종 법안에 합의
2016년 5월	EU 관보(Official Journal)에 GDPR 발표
2018년 5월 25일	GDPR 발효

자료: European Commission 자료를 활용하여 저자 작성.

부록 표 2. 제29조 작업반의 EU GDPR 가이드라인 발간

가이드라인	발표일
영향평가(DPIA) 및 고위험을 유발할 수 있는 개인정보 처리(wp248rev.01)	2017.10.13
개인정보이동권(wp242rev.01)	2017.10.27
DPO(wp243rev.01)	2017.10.30
선임감독기구(wp244rev.01)	2017.10.31
과징금 부과(wp253)	2018.2.13
개인정보 유출 통지(wp250rev.01)	2018.2.13
자동화된 의사결정 및 프로파일링(wp251rev.01)	2018.2.13
규정(2016/679)하 투명성(wp260rev.01)	2018.4.13
규정(2016/679)하 동의(wp259rev.01)	2018.4.16

자료: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360 (검색일: 2018. 5. 4).