

# 2018 개인정보보호 7대 이슈 전망



**DATA PROTECTION BY TRUST,  
TRUST BY DATA PROTECTION**

서로 신뢰하고 함께 보호하는 개인정보



# Contents

## I. 조사개요

## II. 2017 개인정보보호 키워드

## III. 2018 개인정보보호 7대 이슈 전망

- 01 EU, 일반개인정보보호규정(GDPR) 본격시행, 2018년 5월 25일!
- 02 데이터에 미래가 있다. 디지털 경제 시대의 원유, Data!
- 03 Privacy by Design! 개인정보 활용은 정보주체의 안심이 우선
- 04 데이터 무역 활성화! 개인정보 국외이전/데이터 국지화 제도정비 시급
- 05 개인정보 안전한 활용, 4차 산업혁명 선도의 핵심
- 06 사업장 감시 vs 근로자 프라이버시
- 07 바이오정보 빅데이터 시대, 커지는 개인정보 침해 위협



# 조사 개요

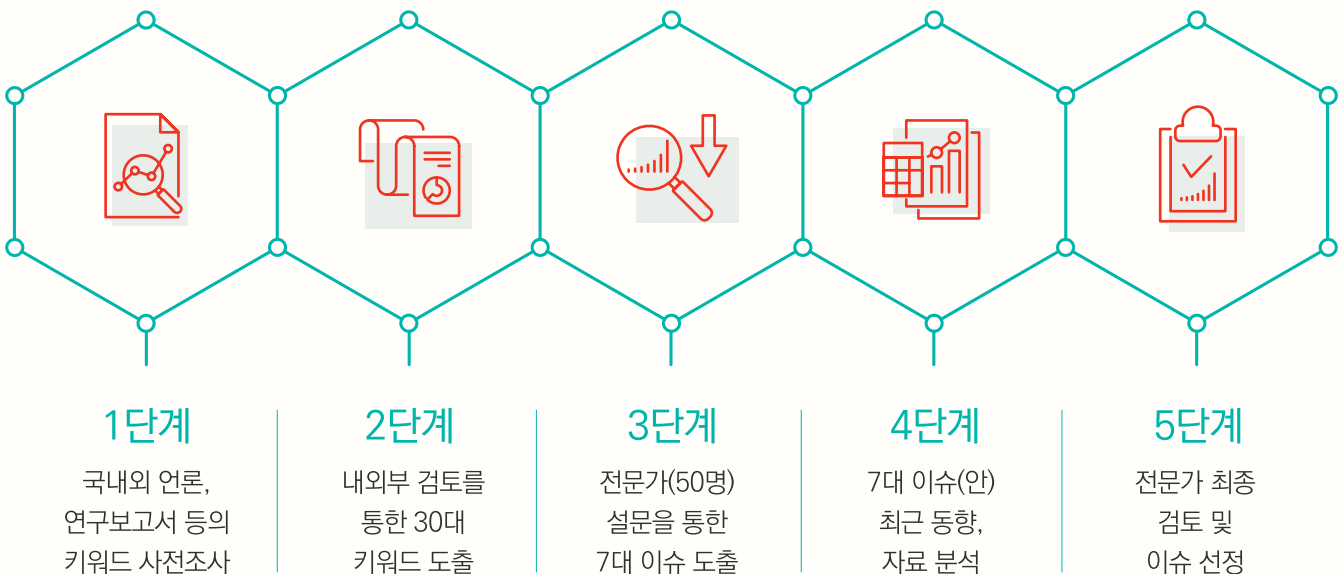
## 조사목적

- 4차 산업혁명 시대에 개인정보 활용의 증가로 개인정보 보호의 중요성도 높아지고 있으며, IT 환경 변화로 인해 새로운 이슈 급증
- 이에 따라, 2018년도 개인정보보호에 있어 중요한 이슈를 선제적으로 제시하여 정책 방향을 수립을 위한 기초자료 확보 추진

## 조사방법

- 국내·외 언론, 연구보고서, 논문(4,064건) 등을 통해 다루어진 개인정보보호 이슈 중 관련 키워드(41,711개) 추출
- 개인정보보호 이슈별 유사성, 중복성 검토 및 최근 동향, 세부 자료분석 등을 통해 중요 키워드(30개) 도출
- 개인정보 전문가(50명) 대상 설문 및 논의 등 거쳐 2018 최종 개인정보보호 7대 이슈 선정 및 전망

## 7대 이슈 선정 절차



# 2017 개인정보보호 키워드

번호	키워드	내용
01	데이터유출/ 정보유출	개인정보 등이 신뢰할 수 없는 환경에 노출되는 것으로, 의도적이거나 의도하지 않은 것 모두를 포함
02	프라이버시 셴드	미국과 유럽연합(EU) 간의 정보 전송협약으로써, 2016년 8월 공식 도입 이후 프라이버시 셴드 준수를 위한 대응 문제가 2017년 상반기까지 꾸준히 이슈화됨
03	정보유출 통지	데이터유출 발생 시 개인 및 관계기관에 통지할 의무
04	e-프라이버시 규정	정보통신망, 정보통신서비스 발달에 적절히 대응하기 위한 목적으로 기존의 전자통신 프라이버시 지침(Directive 97/66/EC)을 대체하여 제정된 EU의 규범
05	데이터 전송	고객 서비스 등을 위해 데이터 센터 또는 제3자에게 고객의 개인정보 데이터를 전송하는 과정에서 개인정보침해 및 동의요건 구성 등 다양한 이슈가 발생
06	얼굴인식	대표적인 바이오인식 기술 중 하나이며 분실이나 복제의 우려가 낮다는 점에서 차세대 신원확인 시스템으로 주목
07	EU 개인정보보호 일반규정(GDPR)	유럽 시민들의 개인정보 보호를 강화하기 위해 제정된 통합 규정. EU 회원국 뿐 아니라, 세계 각국의 개인정보보호 법제의 구성과 방향성을 '현실적으로 구속'한다는 측면에서 주목
08	개인정보 영향평가	개인정보를 처리하는 서비스, 시스템 등의 출시, 개발, 변경 등을 준비할 때 사전에 개인정보보호를 위해 필요한 사항을 검토하는 활동
09	건강정보	전자의무기록(EMR) 도입과 헬스케어 웨어러블 기기 등의 확산으로 개인의 건강정보 공유 및 전송이 활발해지며 프라이버시 침해 우려도 가중
10	개인정보 적용 설계	제품과 서비스, 시스템 등의 설계단계에서부터 개인정보를 보호하고, 이용자의 개인정보 자기결정권과 투명성을 확립할 수 있도록 하는 원칙
11	신원도용	타인으로 가장하기 위해 신분증번호, 운전면허증번호, 신용 카드번호 등 핵심 개인정보를 절취하는 범죄
12	인공지능	머신러닝을 위시한 인공지능 기술을 통해 대량의 데이터를 수집, 분석, 적용하는 과정에서 이용자의 프라이버시를 침해할 가능성도 전례없는 수준으로 고조되고 있음
13	작업장 프라이버시	직원의 이메일계정 감시부터 업무현장의 CCTV 촬영에 이르기까지 작업장에서 온라인-오프라인 사생활 침해 발생
14	동의	개인정보수집, 처리, 이용, 공유 등에 대한 사용자의 동의요건은 opt-in, opt-out 등으로 적용될 수 있으며, IoT 환경 등에서는 동의요건과 방식이 매우 복잡해질 수 있음

15	개인정보 국외이전/ 데이터 국지화	국가 간의 개인정보 수집, 이전, 폐기 등에 따른 프라이버시 침해 방지 논의 활성화. 한편, 기업이 자료를 수집한 국가 안에서만 데이터를 저장하고, 처리해야 한다는 데이터 국지화 원칙도 부각
16	바이오 데이터	지문, 홍채, 얼굴 등의 생체 정보를 활용해 개인을 인증하는 추세가 확산되고 있으며, 정부 차원에서 국민들의 바이오 데이터 DB도 검토 중
17	차등 프라이버시	수집된 데이터에서 집단적 행동 패턴에 관한 유용한 정보를 추출하되, 데이터를 분석하기 전에 임의로 내용을 추가하여 개인정보 노출을 어렵게 만드는 비식별화 기술
18	위치데이터	모바일 기기 등을 통해 IP 주소 데이터를 수집하여 개인의 위치나 거주 지역을 파악할 수 있어 이에 대한 프라이버시 침해 우려 확대
19	데이터브로커	마케팅 등의 목적을 위하여 이름, 주소, 이메일, 특성, 환경, 생활 형태 등 개인 관련 사항을 판매하는 사업자
20	데이터 이동성	이용자의 요청에 따라 특정 기업에서 다른 기업으로 자신의 개인 데이터를 전송할 수 있도록 보장하는 권리
21	데이터 분석	방대한 데이터를 기반으로 유용한 정보를 발견하고 인사이트를 도출하며 의사 결정을 지원한다는 목표로 데이터를 검사, 정리, 변형 및 모델링하는 프로세스
22	스마트시티	첨단 정보통신기술(ICT)을 이용해 도시의 주요 공공기능을 네트워크화 하여 데이터 교환이 활발하게 이루어지는 도시. 데이터 기반의 도시 운용에 따른 프라이버시 이슈 발생
23	감시	사업장, 정부기관 등에 의한 이메일 감청과 온라인 감시, CCTV 등을 통한 근로자 혹은 시민들의 행동과 이동 감시 등이 강화되어 프라이버시를 침해할 우려 고조
24	통신 프라이버시	범죄대응을 위한 수사기관의 통신자료 요청과 통신 및 인터넷 서비스 가입자의 프라이버시 보호를 위한 데이터 공개 거부 의지가 대립하며 프라이버시 공방 전개
25	스마트기기	개인 데이터가 수집 및 저장되는 스마트기기에 바이오인증과 음성인식 등 다양한 기술들이 결합되면서 기기의 분실, 해킹 등에 따른 개인정보 유출과 침해 우려 심화
26	온라인 트래커	사용자들의 온라인 행태 및 웹사이트 방문기록 등을 수집하는 도구들
27	데이터 최소화	개인정보 유출 및 해킹 등에 따른 프라이버시 침해 리스크를 줄이기 위해 개인 데이터 수집 및 보존을 최소화 할 것을 권장하는 원칙
28	비식별화/ 익명화	빅데이터 시대에 개인정보 보호를 위해 개인정보 비식별화 조치 등이 마련되었으나, 법적 근거 미비 등에 따른 쟁점 부각
29	자율주행 자동차	지능형교통시스템(ITS)와 연결된 자율주행차량은 차량의 위치정보를 지속적으로 시스템에 보고함에 따라 사용자의 프라이버시 침해에 대한 우려도 증대
30	데이터보호 책임자	데이터 보호 조치와 관련된 컴플라이언스 업무를 담당하는 직책. GDPR은 반드시 내부에 DPO를 두지 않고 외부전문가도 DPO로 지정할 수 있음. 업무의 독립성 보장

# 2018 개인정보보호 7대 이슈

번호

이슈

01

**EU, 일반개인정보보호규정(GDPR) 본격 시행, 2018년 5월 25일!**

국내 개인정보 법 · 제도와와의 조율 및 기업 등 처리자의 준비 시급

02

**데이터에 미래가 있다. 디지털 경제 시대의 원유, Data!**

디지털 경제의 우위 선점을 위해 데이터 내 개인정보 비식별 이슈 해소 필요

03

**Privacy by Design! 개인정보 활용은 정보주체의 안심이 우선**

개인정보 적용 설계(Privacy by Design) 선진사례 발굴 · 보급을 통한 혁신 유도

04

**데이터 무역 활성화! 개인정보 국외이전/데이터 국지화 제도 정비 시급**

개인정보 국경간 이동 급증, 자국민 개인정보 및 산업 보호 이슈 심화

05

**개인정보 안전한 활용, 4차 산업혁명 선도의 핵심**

서비스별 맞춤형 개인정보 활용가이드 (Code of Conduct) 활성화

06

**사업장 감시 vs. 근로자 프라이버시**

영상정보(CCTV 등) 등을 통한 사업장 감시, 민주적 노사관계의 걸림돌

07

**바이오정보 빅데이터 시대, 커지는 개인정보 침해 위험**

바이오인증, 정밀의료 등 바이오정보 이용 활성화 대비 개인정보 보호 뒷전



## 2018 개인정보보호 7대 이슈



EU, 일반개인정보보호규정( GDPR)  
본격 시행, 2018년 5월 25일!



Privacy by Design! 개인정보 활용은  
정보주체의安心이 우선



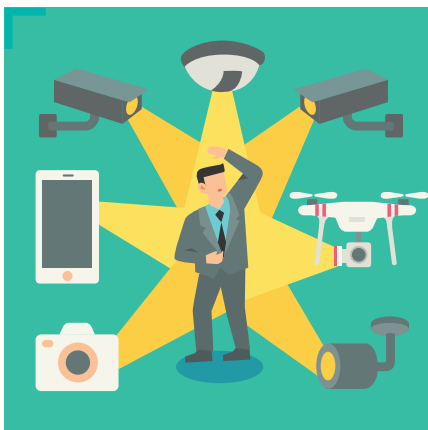
데이터에 미래가 있다.  
디지털 경제 시대의 원유, Data!



데이터 무역 활성화! 개인정보 국외이전/  
데이터 국지화 제도 정비 시급



개인정보 안전한 활용,  
4차 산업혁명 선도의 핵심



사업장 감시 vs. 근로자 프라이버시



바이오정보 빅데이터 시대,  
커지는 개인정보 침해 위험



## 01

2018년  
개인정보보호  
7대 이슈

# EU, 일반개인정보보호규정(GDPR) 본격시행



**유럽연합(EU)의 일반개인정보보호규정(GDPR), 2018년 5월 25일 본격 시행**

국내 개인정보 법·제도와 조율 및 기업 등 처리자의 준비 시급

## 배경 및 현황

유럽연합(EU)의 개인정보 보호법인 유럽일반개인정보보호규정(GDPR-General Data Protection Regulation)이 2018년 5월 25일 본격 시행

- GDPR은 유럽연합 회원국 간에 개인정보의 자유로운 이동을 보장하며 동시에 정보주체의 개인정보 보호권을 강화한 것이 특징

유럽연합 회원국은 GDPR에 부합하도록 자국의 개인정보보호 법령체계를 개편하거나, GDPR 실행하기 위한 사전 작업 진행 중

- GDPR 시행을 앞두고, EU 집행위원회는 전문그룹(Article 29 Working Party 등)을 통해 핵심이슈별로 가이드라인 등(Opinion)을 마련하고 있음

그러나, GDPR의 개별 요구사항을 준수하기 위한 준비 과정에서 제도의 파편화가 확인되고 있으며, 유럽연합 회원국 간에도 실제 GDPR 준비도에 대한 온도차가 상당한 것으로 확인됨

## 이슈

GDPR은 EU 소재 기업은 물론 EU 내에서 사업을 하는 역외 기업에도 적용되며, 위반 시 해당 기업의 유럽 시장 내 사업 제재 및 높은 과징금 적용으로 우리 기업의 우려 증가

신규로 도입되는 정보주체의 개인정보 보호권에 대한 대응 방안이 불확실하며, 특히 감독기관의 법집행 수준에 대한 불확실성이 존재

개인정보 국외이전과 관련, '적정성 평가(Adequacy Decision)' 등 정부차원의 정책적 준비와 더불어 개인정보처리자 및 정보통신서비스제공자의 주의가 필요함

GDPR이 요구하는 개인정보보호 책임자(DPO)를 지정하거나, 국외에서 유럽연합 시민의 개인정보를 처리하는 경우 대리인(representative)을 지정해야 하는 이슈 발생

## 전망 및 대응 방안

- 선임 감독기관(Lead Supervisory Authority)을 조기에 확인, 개인정보처리와 관련한 불확실성 해소 필요
- 정보통신 기업 등이 GDPR의 준수를 위해 적용해야 하는 구체적 서비스 제공 방식에 대해 기술된 한국인터넷진흥원 GDPR 가이드(2017. 12.11 발간) 참고
- DPO의 조기 확보 및 정보주체 권리 보장 방안 마련이 필요하며, 개인정보보호 인증을 조기에 획득하거나 행동강령을 구체화 할 수 있는 사업자 단체의 가입을 고려해야 함
- 유럽연합 역외에서 유럽연합 시민의 개인정보를 처리하는 경우, 대리인(representative)을 지정하는 한편, 위험 관리에 대한 책임을 명확히 해야 함

## 02

2018  
개인정보보호  
7대 이슈

# 데이터에 미래가 있다. 디지털 경제 시대의 원유 Data!



## 데이터가 미래를 결정하는 데이터 경제의 시대 도래

- 데이터 경제의 우위 선점을 위해 데이터 활용의 걸림돌 제거 급선무

### 배경 및 현황

‘데이터(data)’란 사전적 의미로는 ‘정보(information)’ 또는 ‘사실(facts)’, 특히 컴퓨터에서 저장하거나 사용할 수 있도록 한 형태의 정보 혹은 분석 위해 수집된 통계 자료 등을 의미

- 빅데이터(Big data) 관련 데이터의 의미는 기록되거나, 분석되거나 재정리하는 것을 말함

4차 산업 혁명의 가장 두드러진 특징은 ‘데이터의 활용’ 이라고 할 수 있으며, 세계는 지금 데이터 경제(Data Economy) 시대로 접어들고 있음

- 데이터 경제란, 데이터에 접근하고 활용할 수 있도록 협업하는 과정에서 데이터 생산, 인프라 제공, 연구조사 등 서로 다른 역할을 담당하는 구성원으로 이루어진 생태계를 의미

특히, 인공지능 소프트웨어나 프로그램이 하나의 상품 또는 서비스로 탄생하기 위해서 꾸준한 학습 필요

- 인공지능 서비스의 품질과 성능을 높이기 위해서는 보다 많은 양의 데이터와 다양한 종류의 정보가 필요하게 되며, 이러한 학습 과정은 서비스가 개발된 이후에도 계속 필요
- 구글의 알파고(AlphaGo), IBM의 왓슨(Watson for Oncology) 등과 같은 인공지능 서비스는 방대한 양의 데이터 학습을 통해서 탄생
- ※ 인공지능(AI) 바둑 대결 프로그램인 알파고는 세계 최정상 수준의 프로 기사들이 둔 바둑 기보 16만 건에서 추출된 3,000만 수를 학습한 결과 만들어짐
- ※ 인공지능(AI) 암진단 솔루션인 왓슨은 200종 이상의 의학 관련 학술지(저널), 교과서 등을 포함해 1,500만 페이지에 달하는 의료정보를 학습해서 탄생

### 이슈

인공지능 서비스를 위해서는 기존 정보와 자료를 활용한 학습 과정이 필요하므로, 학습용 자료를 수집·이용하는 과정에서 개인정보, 저작권, 영업비밀 등의 침해 이슈가 발생

- 특히 인공지능은 다양한 형태의 정형 또는 비정형 데이터를 모두 처리할 수 있어 개인정보 및 사생활 침해 이슈와 밀접

- 또한 인공지능 학습용 데이터의 생산자(작성자)와 그 학습용 데이터를 활용해서 인공지능 학습을 수행하는 자가 다르다는 것도 저작권 문제를 더욱 복잡하게 만들 수 있음

그러나, 우리나라는 데이터의 활용 사례나 경험이 많지 않아 데이터의 활용에 대한 인식이 낮고 법적 근거도 마련되어 있지 않음

- 오히려 개인정보, 저작권 등의 이용과 활용을 엄격히 제한하고 있는 보호주의적 법제도로 인해 데이터의 안전한 활용조차도 어렵다는 업계 의견 확산

과학연구, 통계작성, 시장조사, 신상품개발 등 목적의 데이터 활용까지 제한하고 있는 관련 법령 개정으로 데이터의 안전하고 생산적인 활용을 보장해야 한다는 사회적 요구 증대

- 우리나라가 4차 산업혁명시대의 낙오자로 전락하지 않기 위해서는 데이터의 활용을 범죄시 하는 환경 개선과 타 국가대비 데이터 활용을 제한하는 법제도 전반에 대한 개정 불가피

특히, 인공지능 학습용 데이터를 포함하여 4차산업혁명의 기반이자 동시에 견인차 역할을 해야 할 데이터 활용에 있어서는 현재 두 가지 방면에서 크게 이슈 제기

- 가명·익명정보의 활용과 저작물의 활용으로 우리나라는 개인정보 활용에 대해서는 소극적 입장을 고수하고 있어 수년째 관련 법 개정엔 진전이 이루어지지 않고 있음

## 전망 및 대응 방안

데이터의 활용이 4차산업 혁명의 성패를 좌우하게 될 것으로 예상되며, 특히 4차 산업혁명시대의 총아로 촉망받고 있는 AI, VR/AR, IoT, 핀테크, O2O, 커넥티드카, 클라우드, 스마트시티 등은 데이터의 활용 없이는 불가능

- 데이터의 양과 품질이 곧 서비스의 품질을 좌우

데이터 활용성 제고를 위해서는 가명·익명정보의 활용을 위한 규제 개선과 저작물의 과학·통계 목적 이용 제한 완화 등의 고려 필요

- 현행법 상 비식별정보(비개인정보)의 이용 및 제공을 금지하는 규정은 없으나, 제한적으로만 허용하고 있어 사실상의 빅데이터 활용에 어려움이 발생할 수 있음
- 전 세계적으로 통용되고 있는 비식별조치 모델들을 참조하여, 「개인정보 비식별조치 가이드라인」을 도입하였으나, 명확한 법적 근거의 마련 등 추가 이슈가 있음

데이터 경제 시대에 대비하여 정보주체의 권리가 침해되지 않도록 보다 안전한 법·제도적 장치를 강구함과 동시에 개인정보의 유용한 활용을 법적으로 보장하는 방안 마련 시급

- 인공지능(AI)의 연구·개발을 촉진하기 위해서는 최소한 저작물을 인공지능 학습용 데이터베이스의 작성에 활용할 수 있게 하고 작성된 데이터베이스를 제한된 범위 내에서 제공 또는 공유할 수 있도록 하는 방안 등도 가능

## 03

2018  
개인정보보호  
7대 이슈

# Privacy by Design!

## 개인정보 활용은 정보주체의 안심이 우선



개인정보 활용 시 정보주체들이 안심할 수 있도록 'Privacy by Design' 적용

개인정보 적용 설계 선진사례 발굴 · 보급을 통한 혁신 유도 필요

### 배경 및 현황

Privacy by Design은 IT 시스템, 네트워크로 연결된 인프라, 그리고 비즈니스 행태의 설계와 운영에 있어 프라이버시 보호를 선제적으로 내재화하는 것에 기초한 프레임워크<sup>1)</sup>

- 해당 개념은 캐나다 온타리오 정보보호위원회, 네덜란드 개인정보보호위원회 및 네덜란드 응용과학 연구기관 등이 1995년도에 발간한 연구보고서("Privacy-enhancing technologies")에서 최초 사용

#### ● 개인정보 적용 설계의 7가지의 기본 원칙 ●

- |  |                            |
|--|----------------------------|
| ① Proactive not reactive – preventative not remedial     | 선제 선제적-사후조치 및 보완이 아닌 사전 예방 |
| ② Lead with privacy as the default setting               | 프라이버시 보호가 가능하도록 기본 설정      |
| ③ Embed privacy into design                              | 설계 자체에 프라이버시 내재화           |
| ④ Retain full functionality (positive-sum, not zero-sum) | 충분한 기능성 유지                 |
| ⑤ Ensure end-to-end security                             | 종단간 보안 확보                  |
| ⑥ Maintain visibility and transparency – keep it open    | 가시성과 투명성 유지                |
| ⑦ Respect user privacy – keep it user centric            | 이용자 프라이버시 존중 – 이용자 중심      |

2018년 5월 시행 예정인 GDPR(General Data Protection Regulation)은 Data protection by design and by default(개인정보보호 적용 설계 및 기본 설정)가 개인정보처리자 및 수탁자의 법률적 의무임을 명시

- '개인정보보호 적용 설계 및 기본 설정'은 개인정보 최소화 및 가명화 방식 등 기술적, 관리적으로 적용 가능한 보호조치를 관련 예시로 언급
- '개인정보보호 적용 설계'의 개념은 개인정보보호 전문가들 사이에 향후 나아가야 할 방향이나 철학으로 이해되었으나, GDPR이 조문에 명문화됨에 따라 구체적인 적용 방안 논의 본격화

1) Deloitte, "Privacy by Design, Setting a new standard for privacy certification", Available at <https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-en-ers-privacy-by-design-brochure.PDF>

## 전망 및 대응 방안

- ‘개인정보보호 적용 설계’는 GDPR을 비롯, 국내 「개인정보 보호법」 등에도 그 기본 정신이 반영되어 있으며, 해당 개념 도입으로 개인정보처리자의 법률준수 의무를 신설하지는 않음
- ‘개인정보보호 적용 설계’는 그 정보시스템에 의해 영향 받는 다양한 이용자, 특히 보호가 필요한 대상의 보호를 강화하는 측면이 있음
- ‘개인정보보호 적용 설계’는 그 자체가 목적이 아니라, 프라이버시 보호 조치의 적용에 그치지 않고 실질적인 ‘결과’에 초점을 맞추어 정보주체의 개인정보 및 사생활을 보호하는 것을 중시 함
- ‘개인정보보호 적용 설계’를 이행함에 있어 기술적, 관리적 보호조치 적용 비용이 발생할 수 있으나, 정보주체의 프라이버시를 보호함으로써 얻는 이익과 신뢰가 더 크다고 볼 수 있음
- ‘개인정보보호 적용 설계’는 개인정보보호를 위한 기술(PETs)의 적용뿐만 아니라, 개인정보를 보호하기 위한 다양한 조직적, 관리적 조치가 적절히 조화되어야 구현이 가능함

### 구체적인 적용방안

- 개인정보 영향평가(PIA, Privacy Impact Assessment) 수행
  - 개인정보를 활용하는 새로운 정보시스템의 도입 및 기존 정보시스템의 중요한 변경 시, 시스템의 구축과 운영이 기업의 고객 등 정보주체에게 미칠 영향에 대해 미리 조사, 분석, 평가하는 체계적 절차
- 프라이버시 중심의 기본 설정 제공
  - 정보주체(이용자)에게 제공되는 서비스의 기본 설정(default settings)이 프라이버시가 충분히 고려된 방식인지를 검토함
- 프라이버시 보호 기술의 적용
  - ‘프라이버시 보호 기술(PETs, Privacy-Enhancing Technologies)’은 정보통신 시스템의 기능을 저하시키지 않고, 개인정보를 제거 혹은 최소화함으로써 불필요하거나 원치 않는 개인정보의 처리를 예방하여 정보 프라이버시를 보호하는 방식
- ”적절한 수준의“ 기술적, 관리적 조치의 적용
  - GDPR은 적절한 기술적, 관리적(조직적) 조치를 적용함에 있어 다음과 같은 사항을 고려하도록 안내함 (Article 25(2))

#### 적절한 수준의 기술적, 관리적 조치 적용시 고려사항

- |                       |                         |
|-----------------------|-------------------------|
| ① 수집한 개인정보의 양(amount) | ② 개인정보 처리의 범위(extent)   |
| ③ 저장 기간(period)       | ④ 접근 가능성(accessibility) |

## 04

2018  
개인정보보호  
7대 이슈

## 데이터 무역 활성화! 개인정보 국외이전/데이터 국지화 제도정비 시급



### 데이터 무역 활성화로 개인정보 국외이전 및 데이터 국지화 논의 활발

개인정보 국경 간 이동 급증, 자국민 개인정보 및 산업 보호 이슈 심화

#### 배경 및 현황

개인정보/프라이버시의 보호와 활용의 균형점이 상이하여 국가별로 관련 규제 상이

- 개인정보의 자유로운 이전을 통한 상품과 서비스 거래의 활성화를 추구하려는 측면과 개인정보의 국외이전으로 개인정보에 대한 통제권이 저하되거나 유출, 오남용되는 등의 위험으로부터 보호를 강화하려는 입장이 양립하여 국가별로 법규제 상이

자국민의 개인정보를 보호하고 외국 사업자의 개인정보 처리에 대하여 집행력을 확보하기 위하여, 주요국은 대체로 개인정보 국외이전에 대한 규제를 강화하는 추세

- 동시에 국가간 개인정보/프라이버시 규제내용과 강도의 불일치를 극복하여 전자상거래 등 서비스의 상호 운용성(interoperability)을 강화하기 위한 노력을 기울여 왔음

한편, 국외이전과는 무관하게 자국 내지 자국 내 특정지역의 규정을 강화하고 해당국에 진출한 기업들에 대한 정보보호 및 개인정보 보호활동을 강화하고 있음

- 따라서, 해당 국가로부터 개인정보를 이전받고자 하는 기업의 준수 부담과 함께 간접적으로 개인정보/정보보호 법제도에 영향력을 미치게 됨
- 대표적인 예로 2018년 5월 시행될 EU의 일반개인정보보호규정(GDPR)과 같이 포괄적이면서도 강력한 개인정보 역외규정을 두는 경우도 있음

또한, APEC의 CBPR처럼 회원국간의 개인정보의 이동을 보다 원활히 하면서 적절한 수준의 개인정보보호가 이루어 질 수 있는 공통된 기준을 정립하려는 노력이 있음

- 2017년 8월 시행된 미국 뉴욕주의 NYCRR500(금융기관에 대한 정보보호규정)처럼 세계 금융의 중심지인 뉴욕에 진출한 상당수의 금융기관들에 대한 법적용이 강제됨으로써 관련 법제도가 사실상 수출이 되는 경우도 있음

한편, 최근 들어서는 개인정보에 대한 국외이전, 역외 적용 분야에서 법규정을 신설하거나 관심을 보이는 국가들이 점차 많아지고 있는 것으로 보임

- 중국의 네트워크안전법, 러시아의 연방법 No.242-FZ와 같은 소위 데이터 국지화(data localization) 이슈가 부각되고 있음

그러나, 데이터 국지화의 실질적인 이유가 정보주체의 이익을 보호 보다는 국가의 개인정보 통제권을 확보하려는 실리가 더 크게 부각되었기 때문에, 기존의 개인정보 관련 법규에 대한 접근법(보호 vs. 활용)과 다른 접근이 필요해 보임



## 이슈

우리나라는 「개인정보 보호법」, 정보통신망법 을 통해 개인정보 국외 전송의 기준을 제시하고 있으나, 관련 실질적 집행 수단의 부재 및 법적 제재규정은 미비

국내 금융회사의 경우 고유식별정보나 금융거래정보, 전자의무기록에 대해 국외이전을 사실상 금지함으로써 일정부분 데이터 국지화 정책을 시행하고 있다고 볼 수 있음

- 따라서 우리 국민의 개인정보 보호 및 집행 가능성 제고를 위한 전략수립 및 대응방안 마련 시급

## 전망 및 대응 방안

국가별로 다양한 형태로 있는 국외 전송을 제한하고 있으며, 해당 국가가 우리나라에 대하여 취하고 있는 정책의 의미와 그에 대한 대응책을 유형화하여 국가별로 대응방안을 강구할 필요가 있음

- 한국은 개인정보 국외 이전과 관련하여 「개인정보 보호법」과 정보통신망법 에서 개인정보를 국외로 이전하기 위해서는 정보주체의 사전동의를 얻어야 한다고 규정하며, 이를 대체할 수 있는 방법에 대한 규정은 없음

EU, 일본 등과 같이 사전동의 이외에 적정성 평가(자국과 동일한 보호수준인지 결정), 국외이전 표준계약, 구속력 있는 기업규칙 제도 도입 등 대안 마련 필요

※ 우리나라는 현재 EU의 개인정보보호 적정성평가(adequacy decision)를 추진 중에 있음

## 05

2018  
개인정보보호  
7대 이슈

## 개인정보 안전한 활용, 4차 산업혁명 선도의 핵심



**4차 산업혁명 시대를 선도하기 위해 개인정보의 안전한 활용 중요성 부각**

서비스별 맞춤형 개인정보 활용가이드(Code of Conduct) 활성화 필요

### 배경 및 현황

사물인터넷 보급 확대에 따른 데이터의 폭발적 증가와 이러한 데이터를 분석하여 활용할 수 있는 인공지능 등 기술 발전으로 데이터를 통해 사회 전 분야에서 다양한 가치가 창출됨

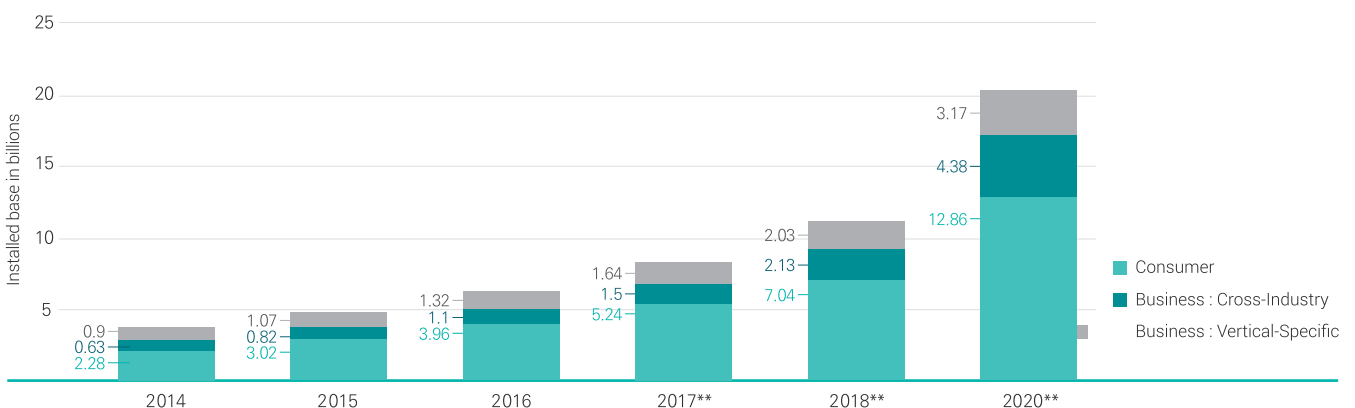
#### ● 대표적인 사물인터넷 구성 기기 예시 ●

- **스마트 가전제품** 스마트TV, 스마트 냉장고, 스마트 체중계 등 백색가전
- **스마트 헬스케어** 심장박동 모니터링 기기, 보행량 측정 및 운동 보조기기, 제세동기 등 삽입형 의료기기
- **스마트카** 인포테인먼트 서비스를 제공하는 커넥티드카(Connected Car), 자율주행차 등 지능형 자동차
- **스마트 제어** 온도조절, 전기절감, 화재탐지와 같은 방재기능을 포함한 자동화된 센서

사물인터넷기기 간 연결 증가로 데이터 생성 폭증할 것으로 예상되는 가운데, IoT 기기의 보안상 취약점을 노린 해커의 개인정보 유출행위도 증가 우려

- '17년도 84억 개에서 '18년도 112억 개, '20년까지 204억 개의 기기 연결 예측

#### ● 사물인터넷 연결 기기 현황(출처 : Gartner, Statista 2018) ●



2025년 전세계 인공지능 산업의 연 매출 규모는 368억 달러로 예측(Tractica)되는 등 인공지능의 활용 보편화 추세 뚜렷

- 인공지능은 주식트레이딩, 개인 신용평가 등 금융 분야, 맞춤형 치료·진단 등 의료분야, 가정의 인공지능스피커, 홈비서 등 스마트홈 서비스 보급 확대 예상

국내는 평창올림픽을 계기로 3단계 수준의 자율주행시스템 기술이 시연될 예정이며, 미국의 테슬라와 GM은 3단계 수준의 자율주행차 양산화 예정

## 이슈

알고리즘의 복잡성, 방대한 데이터의 처리 심화로 정보주체는 자신의 개인정보를 언제, 어떻게 수집하고, 생성하는지 등의 처리과정 파악이 어려워짐

인공지능, 사물인터넷 서비스를 위해서는 취미, 혈액형, 주소 등 정적 정보와 구매패턴, 서비스 이용현황 등 동적인 개인정보가 수집·활용됨에 따라 개인정보 유출 위험도 증가

- 특히, 예측할 수 없는 경로로 개인정보가 유출될 가능성이 높아 주의 필요

자율주행차는 운행과 탑승자의 편의를 위해 실제 방대한 양의 정보를 실시간으로 수집하여 처리하는 거대한 네트워크 기기임

- 이러한 특성으로 인해 상시 외부와 연결되어 있어 해킹과 같은 악의적인 침해가 이루어질 경우 경제적 손실 뿐만 아닌 인명피해도 수반

이와 같은 신기술은 실시간으로 정보주체와 제3자의 개인정보 처리가 필요하나, 현행 법률은 정보주체의 동의 등 엄격한 처리요건 등이 걸림돌이 될 수 있음

- 법과 기술 현실 간 괴리 해소를 위한 개인정보보호 관련 법 정비의 요구가 지속될 것으로 예상

## 전망 및 대응 방안

주요국가들은 이러한 데이터 기반 디지털 경제에서 주도권을 확보하는 한편 개인정보 보호를 위해 개인정보 보호관련 법·제도를 정비하고 있음

법과 기술 간의 간격을 해소하기 위해 정보처리의 투명성 강화와 더불어 위험 기반 접근의 법제 개선, 정보처리자의 책임성 강화, 개인정보 활용의 유연화 필요

- 인공지능의 복잡·다양한 개인정보처리 환경에서 개인정보가 어떻게 수집·이용·제공 등 처리되는지를 알고 통제할 수 있도록 고지제의 실효성 확보 등 투명성 강화가 필요
- 개인정보보호 규제는 개인정보의 성격, 위험도 등을 고려한 위험 기반의 접근이 필요하며 개인정보처리자의 책임성을 강화할 필요(PbD, 개인정보보호 영향평가제도 확대 등)
- 개인정보의 수집·이용 요건에 대한 해석기준 마련하여 개인정보처리자가 개인정보 처리의 유연성 확보 및 형식적 동의 관행 타파로 정보주체의 실질적 권리를 보장할 필요가 있음

## 06

2018  
개인정보보호  
7대 이슈

## 사업장 감시 vs. 근로자 프라이버시



### 사업장 감시와 근로자의 프라이버시 침해 문제 상충으로 관련 민원 급증

영상정보(CCTV 등) 등을 통한 사업장 전자 감시, 민주적 노사관계의 걸림돌

#### 배경 및 현황

■ 근로자들 사이에 개인정보권에 대한 인식이 확산되면서 사업장 전자감시 전자감시와 관련한 민원 급증

※ 국가인권위원회에 접수된 사업장 전자감시 관련 진정과 민원은 2011년 33건에서 2012년 73건으로 급증한 뒤 매년 70건 가량을 유지하다가 2015년 101건으로 증가

■ 노사관계의 특성상 근로자들이 전자감시에 의한 피해에 대해서 공식적으로 문제를 제기하기는 현실적으로 어려움

※ 2013년 인권위 '정보통신기기에 의한 노동인권 침해 실태조사' 결과, 사업장 전자감시로 개인정보를 침해당한 경우 공식적으로 문제제기했다는 응답자는 28.4%에 불과

■ 국가인권위원회는 기업들이 폐쇄회로(CCTV)와 위치확인시스템(GPS) 등을 이용해 사업장에서 직원들의 행동을 무분별하게 감시하는 관행을 엄격하게 규제할 것을 촉구

● 또한, 고용노동부의 인사·노무 분야 '개인정보 보호 가이드라인'에 사업장 전자감시의 주요 유형별 개인정보 처리 요건 및 절차, 근로자 권리보호 등 사항을 구체적으로 명시하도록 권고

#### 이슈

■ 첨단 감시장비의 대중화로 인한 사용자들의 전자감시는 더욱 확대될 것으로 예상되며, 이에 대한 근로자들의 불만과 불편도 점차 증가할 것으로 예상됨

■ 대다수 사용자(고용주)들이 전자감시를 범죄나 범위반으로 보고 있지 않으나, 현행법상 사업장 내 전자감시는 명백히 범죄 행위에 해당

■ 사업자가 전자감시 활동에 대해서 문제의식을 가지고 있는 경우에도 범죄예방, 시설보호, 화재예방, 사이버보안 등으로 용도를 위장하는 경우가 있음

■ 사업장 내 CCTV 설치·운영시 원칙적으로 정보주체(근로자 등)의 동의를 받아야 하나, 노사관계라는 특수한 성격 때문에 근로자의 고용주 동의 요구 거부 사실상 불가능

또한, 사업장 전자감시 유형에 따라 적용받는 법이 다양하여 근로자는 물론 사업자들도 현황을 파악하고, 적절한 대응을 하는데 있어 어려움 발생

● 사업장 전자감시의 유형 및 관련 법 ●

전자감시 유형	관련 법 및 조항
CCTV 등 영상정보처리기술에 의한 감시	▶ 「개인정보 보호법」
이메일, 전화도청 등에 의한 감시	▶ 통신비밀보호법
컴퓨터 감시	▶ 정보통신망법, 형법
GPS 등에 의한 감시	▶ 위치정보법
지문 · 홍채 · 정맥 등 출입통제 시스템에 의한 감시	▶ 위치정보법

## 전망 및 대응 방안

사업장 내 전자감시 남용에 따른 노사분쟁을 줄이기 위해서는 사업장 내 전자감시 장비 도입의 목적, 절차 및 방법에 있어서 투명성 보장 필요

우리나라도 「근로자참여 및 협력증진에 관한 법률」에서 ‘사업장 내 근로자 감시 설비의 설치’를 노사협의회의 협의 대상으로 열거(제20조 제1항 제14호)하는 등 관련 내용을 규정하고 있지만 사실상 역할을 하고 있지 못해 대응방안 마련 필요

- 또한 근로자 감시 설비의 설치에 대해 노사협의회 협의를 거치지 않더라도 이를 강제하거나 처벌할 수 있는 규정이 없고, 협의 논의 결과에 대한 구속력도 규정되지 않음

따라서, 우리나라도 사업장 감시 목적으로 이용될 수 있는 장비나 설비를 도입할 때에는 그 용도에 관계없이 근로자 대표기관에 사전에 충분한 자료를 제공하여 설명 하고 설치의 시기, 방법, 장소, 범위, 용도 등에 대해서도 협의 의무 적용 필요

사용자가 이와 같은 절차를 거치지 않거나, 회피하거나, 불성실하게 대응한 경우에는 이를 강제할 수 있는 절차를 도입하고, 최종적으로 근로자들의 단체법적 동의를 받게 하거나 최소한 노사협의회의 의결을 거치도록 하는 방안 검토

## 07

2018  
개인정보보호  
7대 이슈

# 바이오정보 빅데이터 시대 커지는 개인정보 침해 위협



## 바이오정보 빅데이터 시대가 도래하면서 개인정보 침해 위협이 커지고 있음

바이오인증, 정밀의료 등 바이오정보 이용 활성화 대비 개인정보 보호 뒷전

### 배경 및 현황

과거에는 바이오정보가 병원이나 수사기관에서만 제한적으로 사용되어 왔으나 최근 IT기술과 결합하면서 바이오정보의 용도가 다양해지고 사용 빈도도 폭발적으로 증가

- 금융회사와 휴대전화, 출입통제시스템 등을 생산하는 IT회사 등으로까지 활용이 확대되었으며, 웨어러블 단말기 제조사, 스포츠 업계, 대학, 연구기관 등에서도 바이오정보 관심 증대

바이오정보의 범위도 과거에는 지문, 사진, 디엔에이(DNA) 정도였으나 오늘날에는 사람의 거의 모든 생물학적·신체적 특징과 행동적 특징까지도 개념에 포함시키는 경우가 있음

- 예컨대 지문 외에 홍채, 혈관 형태, 얼굴 형상, 음성, 망막, 손 모양, 손가락 모양, 열상, 성문, 유전자 등외에 개인의 걸음걸이, 필적, 키보드 타이핑, 입술 움직임 등

금융결제원이 추진하는 금융권 공동 생체(바이오)인증·FIDO(Fast Identity Online) 시스템이 본격 가동되면서 바이오정보 유출이 우려되는 상황

- 바이오정보 보호를 위해 바이오정보를 분할하여 일부는 금융사 서버나 이용자 개인단말기(매체)에, 일부는 제3의 기관인 금융결제원 분산관리센터에 각각 보관하는 분산 관리 추진 중

한 편, 정부는 '국가전략 프로젝트' 가운데 하나로 정밀의료를 인공지능 등과 함께 선정하고 집중적으로 육성하겠다고 밝힘(2016년 8월 대통령 주재 과학기술전략회의)

- 정밀의료를 위해서 유전자와 환경이 특정 질병과 어떤 연관성을 보이는지에 대한 선행 연구용으로 충분한 참여자들의 각종 자료를 모은 데이터베이스 구축 예정

### 이슈

바이오정보는 정보주체 또는 이용자가 굳이 머릿속에 이를 기억하지 않아도 되고 별도로 기록해 둘 필요가 없다는 점에서 기억 및 휴대의 편의성 때문에 그 수요와 이용이 급증

- 그러나, 바이오정보만이 가지고 있는 유일성과 고유성 때문에 한 번의 유출시 정보주체에게 영원히 회복할 수 없는 피해를 남게 되며, 해당 바이오정보는 더 이상 활용 불가

- 또한 바이오정보에는 그 사람의 건강 상태나 유전적 내력까지 알 수 있는 다양한 정보가 들어 있어 매우 민감하고, 오남용시 사회적 차별이 발생할 수 있음

■ 또한, 바이오정보의 독점도 개인정보를 이용한 차별을 야기할 수 있어 심각한 경제·사회적 문제를 가져올 수 있음

- 예컨대, 보험회사가 바이오정보를 수집하여 무절제하게 보험요율 등의 산정에 활용한다면 사회적 저항에 직면할 수도 있음

■ 그럼에도 불구하고 바이오정보의 수집·이용 및 제공에 대해서는 현재 개인정보보호 관련 법령에만 의존하고 있고, 다른 별도의 보호 장치는 마련되어 있지 않음

- 단, 바이오정보 중 바이오인식정보와 관련하여서는 '바이오정보 보호 가이드라인(방송통신위원회/한국인터넷진흥원, '2017년 12월 발간)'을 통해 규범적·기술적 보호조치가 제시되어 있음
- 개인정보 보호 관련법에서는 바이오정보도 다른 개인정보와 같이 취급하고 있고, 고유식별정보 수준에서 특별히 더 보호하거나 더 강화된 처리원칙을 적용하고 있지 않음

## 전망 및 대응 방안

■ 사물인터넷(IoT), 인공지능(AI) 등 IT기술의 증가와 핀테크, 전자금융 등의 이용 확대로 바이오정보의 수요는 폭발적으로 증가할 것으로 보임

■ 바이오정보의 위험성과 민감성에 비추어 바이오정보의 활용에 대한 명확한 근거 필요

- 현재 바이오정보는 개인정보의 일부로써 「개인정보 보호법」, 「정보통신망법」, 「신용정보법」 등 개인정보 관련법령에 의해서 보호를 받고 있고, 유전정보는 민감정보로 보호받고 있음
- 그러나, 유전자정보 수집·이용시 정보주체의 별도 동의 조항 및 바이오정보 수집·전송시 암호화 의무 정도의 일반적 규정만 존재

■ 바이오정보에 대해서는 법률에서 정의부터 명확히 규정하여 일반 개인정보보다 더 강화해서 보호해야 할 대상과 범위가 무엇인지부터 명확히 해야 함

- 이를 위해서는 우리나라에서 구분해서 사용하고 있지 않은 바이오정보와 바이오인식정보의 차이부터 명확히 제시하여야 함
- 지문, 얼굴사진, 홍채, CCTV 등을 통해서 촬영된 개인영상정보, 콜센터 녹음된 목소리 그 자체와 그로부터 추출된 바이오인식정보를 모두 바이오정보로 규정할지 여부 논란
- IoT 단말기를 통해서 수집된 혈압, 심박수, 당뇨수치, 수면상태 등을 바이오정보의 개념에 포함할지, 의료정보로 별도의 법률 또는 규정 등으로 구분해서 보호할 것인지도 논의 필요

- 본 보고서 내용에 대해 무단전재를 금하며, 가공 · 인용할 때는 반드시 출처 「한국인터넷진흥원」을 밝혀주시기 바랍니다.
- 본 보고서의 내용은 행정안전부 · 한국인터넷진흥원 공식 견해와 다를 수 있습니다.







---

## 2018 개인정보보호 7대 이슈 전망

---