개인정보보호규칙과 실무사례

2016. 11. 25.

삼성전자 법무실
김도엽 변호사

※ 본 강의자료는 강의 목적으로 작성하였으며, 삼성전자㈜의 공식 입장과 무관함을 알려드립니다.

Table of Contents

1. 배경

2. 주요내용

3. 전망 및 대응

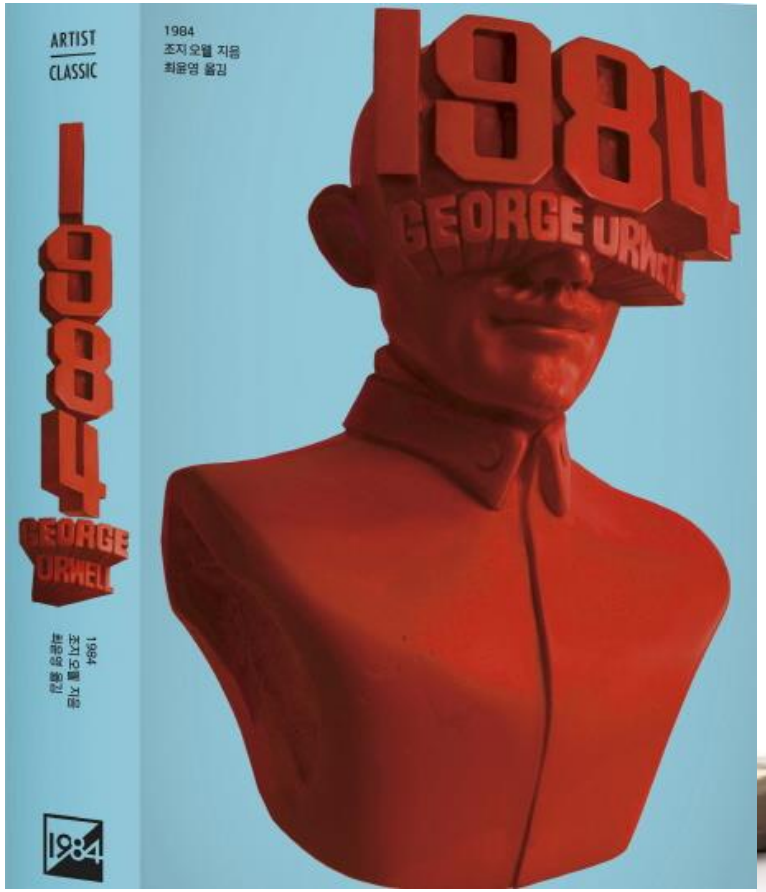
소개

- 대한변호사협회 IT 전문, 방송통신 전문변호사
- 행정자치부 장관 표창 수상
- 행자부 개인정보 민관협력포럼 위원
- 방통위 APEC CBPR작업반
- EU 적정성 평가 민관 합동 추진단 위원
- ISO 27001 Auditor/Lead Auditor
- 개인정보영향평가(PIA) 전문인력
- PIPL , PIMS 개인정보 인증심사원
- SECU-STAR 정보보호준비도 평가사
- 개인정보보호전문강사(KISA)
- 평창동계올림픽 정보보호 전문위원회 자문

1

배경

1984


ARTIST
CLASSIC
1984
조지 오웰 지음
최윤영 옮김
1984
GEORGE URWELL
1984


hello.

1980 OECD

(Organization for Economic Co-operation and Development)

1980년 9월 이사회 권고
프라이버시 보호 및
개인정보의 국가간 이전에 관한 가이드라인

1980 OECD 가이드라인 제8원칙

- Collection Limitation Principle
- Data Quality Principle
- Purpose Specification Principle
- Use Limitation Principle
- Security Safeguard Principle
- Openness Principle
- Individual Participation principle
- Accountability Principle

1980 OECD 가이드라인 기본원칙

- 회원국은 프라이버시와 개인자유의 보호라는
  명목 하에 보호에 필요한 조건을 벗어나는
  국제간의 유통을 방해하는 법, 정책 및 활동의 개발을
  피해야 한다.

- 회원국은 회원국과 비회원국간의
  개인데이터의 국제적인 유통을 제한하는 행위를
  삼가야 한다.

EU Directive

1995년 개인정보 보호지침(95/46/EC)
정보이전의 제한

12年 GDPR案
(General Data Protection Regulation)

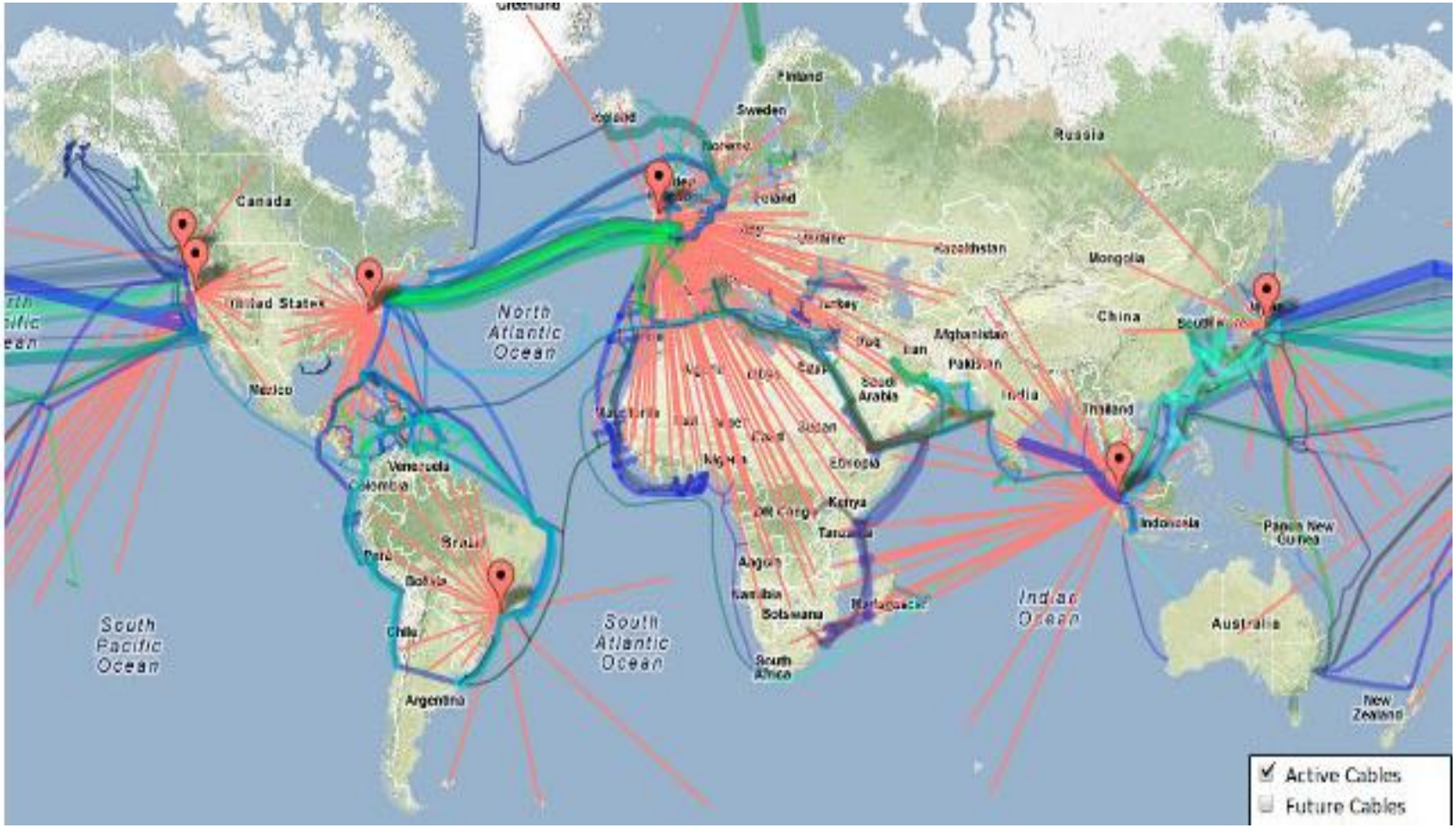
개인정보의 처리와 관련된
개인의 보호 및 개인정보의 자유로운 이동에 관한 규율

2013 OECD 가이드라인 기본원칙

- 회원국은 다음 중 어느 하나의 경우에 외국과의 개인정보의 국가간 이전에 대한 제한을 억제해야 한다
  - 해당 해외 국가가 가이드라인을 준수하는 경우
  - 충분한 Safe Guard 가 존재하는 경우

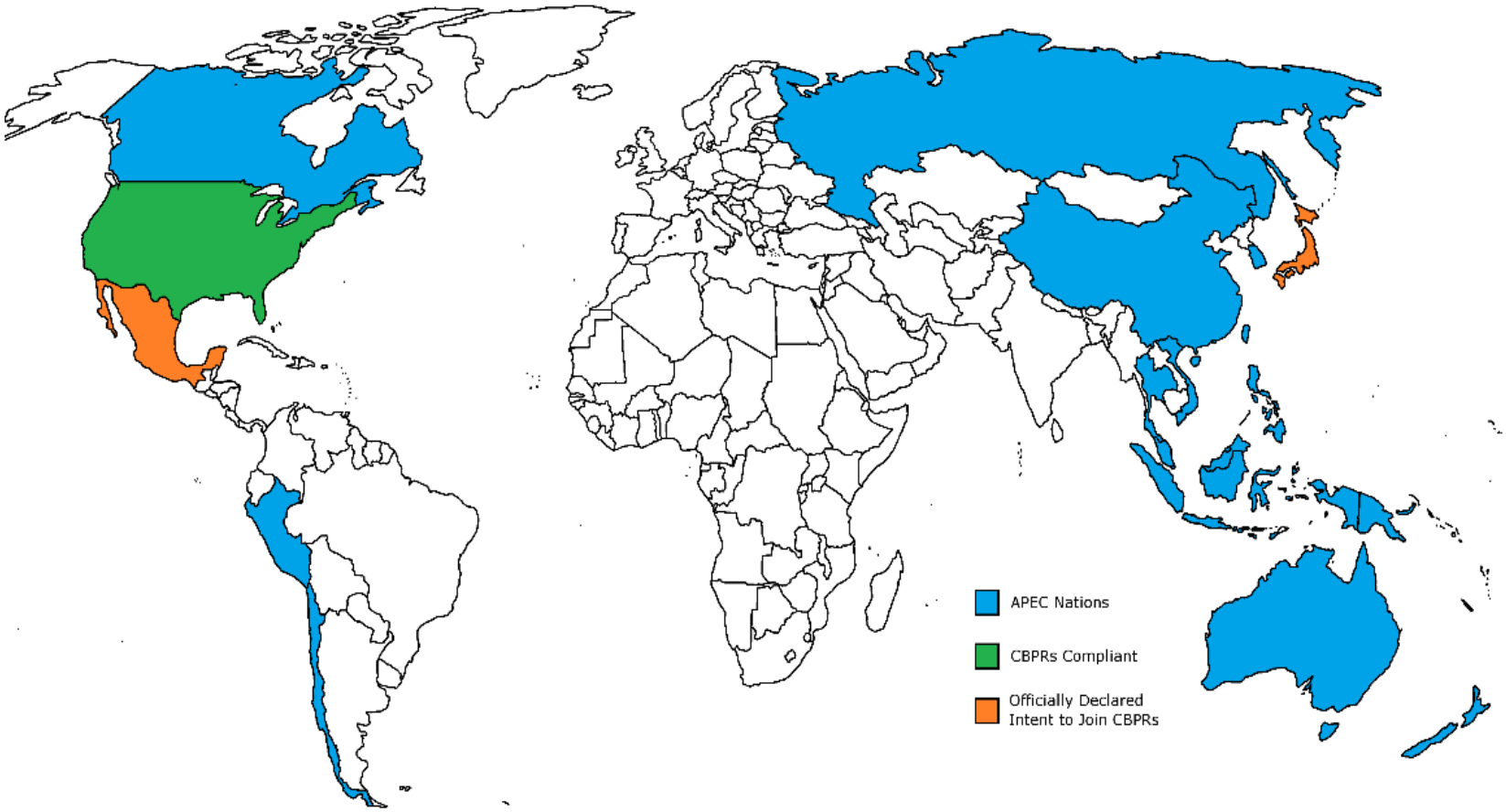
- 국가간 개인정보의 이전에 대한 제한은 처리의 목적, 맥락, 해당 정보의 민감성을 고려하여 제시된 위험에 적절한 것이어야 한다.

현재는...


Canada
United States
Mexico
Venezuela
Colombia
Brazil
Peru
Bolivia
Chile
Argentina
North Atlantic Ocean
South Pacific Ocean
South Atlantic Ocean
Indian Ocean
Finland
Sweden
Norway
Poland
Ukraine
Russia
Kazakhstan
Mongolia
China
Turkey
Iran
Afghanistan
Pakistan
India
Saudi Arabia
Egypt
Libya
Algeria
Sudan
Nigeria
Ethiopia
Kenya
Tanzania
Angola
Namibia
Botswana
South Africa
Thailand
Indonesia
Papua New Guinea
Australia
New Zealand
Active Cables
Future Cables

APEC- CBPRs

(Cross Border Privacy Rules)



CBPR
(Cross Border Privacy Rules)

장점	단점
APEC 국가에서의 비즈니스 운영 Risk 완화	신규 프레임워크로 APEC 국가들의 지원을 받고 있으나, 아직 소수국가만 승인을 취득
APEC 국외전송 요구사항을 준수	

Privacy Shield

U.S.★EU

SAFEHARBOR

U.S. DEPARTMENT OF COMMERCE

NSA가 이렇게 궁지에 몰리게 된 가장 큰 장본인의 거취
그의 귀국을 요청하는 글들이 다수의 소셜 사이트에 공유

[보안뉴스 주소형] 미국 국가안전보장국인 NSA가 처음으로 궁지에 몰렸다. 미국 현지 시간으로 지난 7일, 미국 연방법원에서 NSA의 도청을 통한 정보수집 수준이 애국법(Patriot Act)에 위반될 수준의 도를 넘어섰다고 2심 판결을 내린 것. 사실 NSA가 해당 문제로 법정에 선 적은 수차례 있었지만 미국 법원이 NSA의 손을 들어주지 않은 것은 이번이 처음이다.

※ 출처:보안뉴스, 더 가디언 유투브 인터뷰

⇒ Schrems 판결 이후 Privacy Shield 도입

현재는…

- **개인관련 정보가 다수 발생**
  (전체 데이터 70%, ICD, 2011)

- **전세계 데이터의 90%**
  최근 2년간 만들어진 것(인포그래픽)

- **Mega Trends**
  - **Big Data**
  - **IOT**

    (1조 2000억 달러: 22년)
  - **Cloud**

⇒ 개인정보보호에 대한 신규 프레임 필요

2

주요내용

GDPR
(General Data Protection Regulation)

- Directive 이후 변화된 인터넷 기술과 환경 변화를 반영

- 4년간의 합의 과정, 3000건 이상 수정안 제출

- 적용범위 확대, 막대한 처벌

- 공표일자: 2016. 5. 4.
  발효일자: 2018. 5. 25

Directive와 Regulation

- **Directive**
  - Directive 내용에 따른 별도의 입법행위 필요
  - 각 개별 국가 법령의 차이가 있음(영국, 독일)

- **Regulation**
  - 별도의 입법행위가 불필요함
  - 하나의 법령으로 전체 국가에 적용

⇒ 회원국가의 상이한 제도를 단일 형태로 통합하고
보다 강력한 규제를 시행할 것으로 예상
단, 가이드라인/집행사례 등이 미확정, 현재 규정을 바탕으로 검토

개인정보의 범위 확대

- 최근 유럽사법재판소(CJEU)의 10/19日 판결에 따르면,
  Directive에 따르더라도 유동 IP의 개인정보성 인정

- 특히, GDPR Article 4 (1)에서는 식별자(Identifier)의 개인정보성을
  명시적으로 규정하고 있으므로, DUID, S/N 등
  다양하게 사용되는 식별자의 개인정보성이 인정될 것으로 예상

적용대상

- 기존 EU directive는 EU 內 설립(establishment) 또는 설비(equipment)를 기준으로 판단

- 신규 GDPR은(Article 3)은
  - 법인이 EU 내 설립한 경우는 물론,
  - EU Residents에게 제품이나 서비스를 제공하는 경우
  - EU Residents의 행동을 monitoring 하는 경우에도 적용

⇒ 구주에서 사업을 하는 대부분의 대한민국 기업은 적용 대상

처벌조항

- **기존 대비(영국: 최대 50만 파운드) 막대한 제재금**

  - 행태 별로 최대 전세계 매출의 2 ~ 4% 또는
    10M ~ 20M 유로 제재금 부과

  - 4%, 20M유로 : 국외전송, 정보주체 권리보장 等
    2%, 10M유로 : Child Consent, Data Protection by Design 等

Accountability

- Data Protection Officer 선임 (Art. 37)

- 주요 업무

  Core activities
- 대량의 개인정보를 처리하는 경우

  On a Large Scale
- 사외 DPO 가능

⇒ 국내 개인정보보호책임자와 유사한

구주 DPO 선임을 고려해야 하며, 실질적인 업무를 수행

Accountability

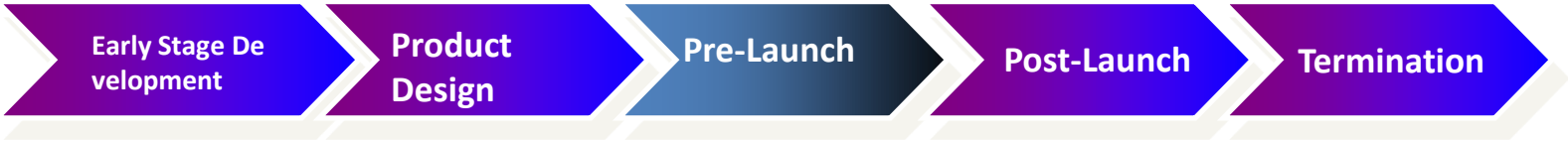
- **DPO의 지위**
  - DPO는 독립적으로 활동
  - 경영진에게 보고할 수 있는 지위

- **DPO의 의무**
  - 개인정보보호 관련 자문
  - 개인정보보호 의무 이행 모니터링
  - 규제기관, 정보주체의 Contact Point로 역할
  - Privacy by Design 자문
  - DPIA(Data Protection Impact Assessment) 자문 등

Accountability

Privacy by Design(Art. 25)

- 신규 기술, 서비스, 제품을 출시할 경우 개인정보보호
- 라이프 사이클 별 검토(기획 – 개발 – 운영 – 종료)



Check list

- Early stage Design Checklist
- Pre-launch Product Design Checklist
- Active Product or Service Checklist
- Product Termination Checklist
- Material Change Checklist
- Third party Sharing Checklist
- EU data Transfer Checklist

Accountability

Privacy by Design(Art. 25)

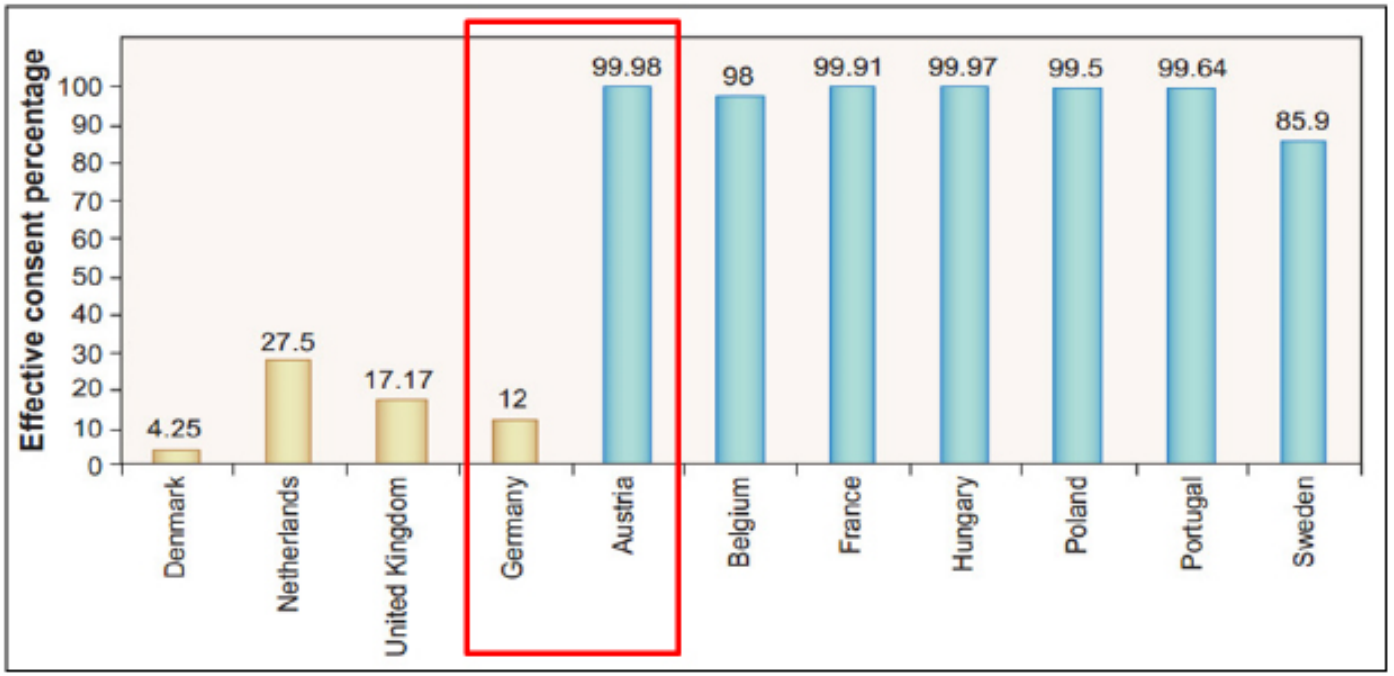
- **Review Process**
  - 시스템화
  - 강제화

- **Privacy Dash Board**
  - 각 단계별
    현황 모니터링

Accountability

Privacy by Default(Art. 25)

- 필요한 목적 범위 내에서만 제한적 개인정보 처리



※ 출처: Johnson, E. J. & Goldstein, D. G. (2003). Do defaults save lives? Science, 302, 1338-1339.)

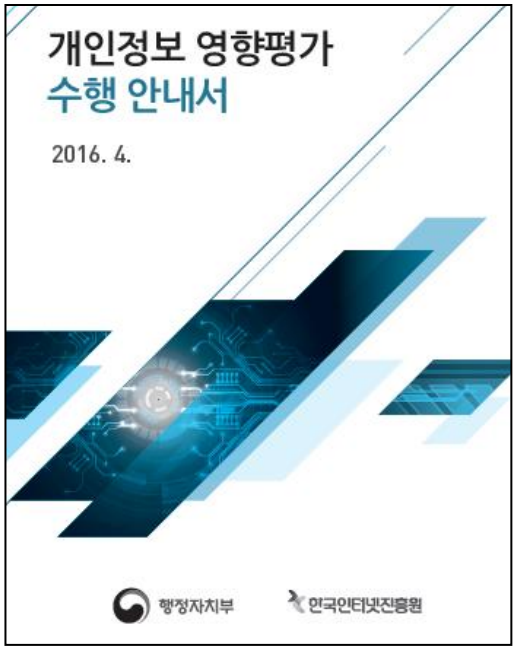
Accountability

Data Protection Impact Assessment(Art. 35)

- 개인정보를 처리하기 전에 사전 영향평가
- 개인의 권리와 자유에 대한 심각한 위험이 있는 경우
- 대량의 정보, 민감한 정보, 개인에 대한 평가 정보

※ 국내에는 개인정보보호법상 공공기관에 의무 부여 中
ISO 기준 가능성도 大

⇒ 지속적인 규제기관 모니터링,
필요 時 대상시스템 개인정보 영향평가 수행



정보주체의 권리 강화

Access and Objection Right(Art. 15, Art. 16, Art. 21)

- 정보주체의 개인정보 접근권
- 개인정보 수정
- 개인정보 처리금지

정보주체의 권리 강화

Right to be forgotten(Art. 17)

- CJEU의 Costeja vs Google 판결

- 정보주체는 자신의 정보를 처리하는 Data Controller에게 Link, copy 또는 replication에 대한 삭제요청 가능

정보주체의 권리 강화

동의

- a freely given, specific, informed and unambiguous indication

※ 동의의 자발성, 유효성 문제

정보주체의 권리 강화

Portability(Art. 20)

- **해당 법령에 포함될 수 있는 데이터의 범위 산정**
  - ISP가 보유하고 있는 Data, Telemetry Data, 시장조사데이터, E- Retailer가 보유한 Data 等
  - Controller의 투자 수준, 지적 재산권 침해 고려

- **이용자가 제공한 정보범위**
  - SNS, IOT 데이터 등 범위에 대한 논의 확대

- **일반적으로 통용될 수 있는 데이터 포맷**
  - 포맷의 호환성, open 포맷의 사용가능성 고려

※ 의료 서비스, Cloud 서비스

정보주체의 권리 강화

Profiling(Art. 22)

- **대부분의 다른 국가에는 현재 도입되지 않은 개념**
  - 자동화된 정보처리를 통해
  - 정보주체의 선호도, 행동 양식을 분석하여,
    정보주체에게 영향을 미치는 경우

- **이유**
  - 기술 발전으로 인해
    소비패턴, 관심사, 선호도 등을 통해 정보주체를 분석할 수 있고,
    향후 행동도 예측 가능

예시)
급여, 주거지 , 건강상태, 정치적 성향, 관심사, 학력, 직업 등을
결합하여 분석할 경우 프로파일 생성 가능

정보주체의 권리 강화

Profiling

- 원칙적으로 정보주체에게 프로파일링을 거부할 수 있는 권리를 부여

- 단, 예외적으로
  계약의 이행
  규제기관의 승인
  명시적인 동의가 있는 경우 프로파일링이 가능

⇒ **Profiling에 해당하는 지 여부 판단 필요**
실무적으로 적법하고 유효한 동의를 받는 방법 검토 및
이용자가 실질적인 혜택을 얻을 수 있는 서비스를 제공

개인정보 유출 신고 및 통지

Data Breach Notification(Art. 33 & 34)

- **원칙:**
  - 정보주체에게 영향을 미치지 않을 경우: 규제기관에 신고
  - 정보주체의 권리와 자유에 영향을 미칠 경우: 정보주체에게 통지

- **규제기관**
  - **통지항목:**
    정보유출의 성격(유출 수, 유출종류, 유출의 범위 等)
    DPO Contact point
    유출결과
    유출 대응을 위한 조치

  - **통지기간**
    72시간 內(국내 정보통신망법은 24시간 內)

개인정보 유출 신고 및 통지

Data Breach Notification(Art 33 & 34.)

- 정보주체

- **통지항목**
  정보유출의 성격
  DPO Contact Point
  피해 최소화를 위한 조치 등
- **통지기간**
  지체 없이
- **예외**
  적절한 수준의 보호조치가 취해진 경우 등
  ※ 유출정보가 암호화된 경우

⇒ 유출신고 대응 계획을 사전에 작성하여
사고 발생시 신속하게 대응할 수 있도록 준비가 필요

One Stop Shop

One Stop Shop(Art. 56, 63 ~67)

- EU 국가에 다수의 법인을 설립한 경우
  하나의 법인이 다수 국가의 정보주체의 개인정보를 처리하는 경우 등
  하나의 Lead Authority의 규제를 받음

- Lead Authority는 One Stop Shop으로서,
  개인정보처리 프로세스를 감독할 수 있음

- 단, 다수의 국가에 영향을 미치는 개인정보 처리에 대해서는
  관련 규제기관의 컨설팅을 받아야 함 (예컨대, BCRs)

역외 전송

개인정보의 역외전송(Art. 40 ~ 44)

- 명시적인 동의(Consent)
- 계약관계(Data Transfer Agreement)
- 적정성 평가(Adequacy)
- 구속력 있는 기업 규칙(Binding Corporate Rules)

대응방안

- **장기적인 방안**
  대한민국의 적정성 승인 추진

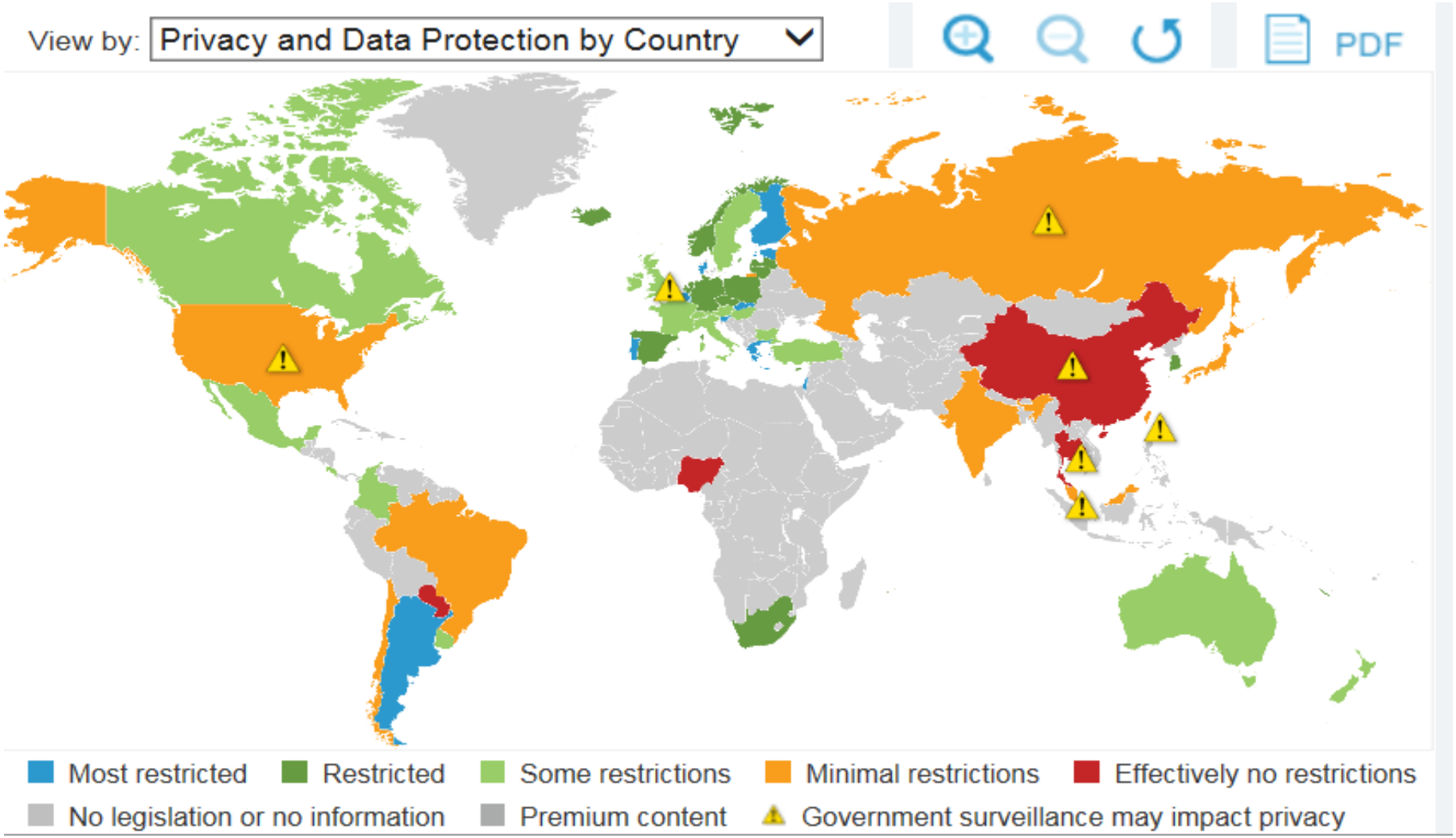
- **중단기적인 방안**
  정보주체의 동의 및 법인간의 계약 추진 또는 BCR 고려

3

전망 및 대응

현재는...

Forrester's 2016 Data Privacy Heatmap Points To Continued European Influence On Global Regulations ※ 출처: Forbes



※ 출처: http://forrestertools.com/heatmap/

현재는…

- **세계 여러 국가들이 유럽 기준을 근거로 변경 中**
  - 일본의 개인정보보호위원회 설립

- **실제로 유럽연합 뿐만 아니라 역외 국가들의 입법도 진행**
  - 한국: 관련 매출 3% 규정

- **정부기관의 감시활동이 강화에 대한 시도가 확대**
  - 독일, 네덜란드 등

※ 출처: Forbes

전망 및 대응

- **명목적인 법령이 아닌 실제 집행 가능성** 大

  약 2년간의 유예기간 이후 즉시 발효

- **사전 대응 조치 필요**

  WP의 가이드라인 모니터링

  시스템 및 서비스에 대한 사전적, 예방적 준비작업을 진행 필요

  ※ 미국 기업, 다양한 방법으로 방어 체계 구축 中

- **민·관 협력을 통한 중소기업, 스타트업 지원**

Thank you.

김도엽 변호사
doyeup.kim@samsung.com
+82 10 8639 5565