RETURN VALUES

GDPR의 이해와 대응방안

Dec. 2018

RETURN VALUES

Agenda

I. GDPR

II. 적용범위

III. Controller & Processor

IV. GDPR에서 규정하는 개인정보

V. GDPR과 블록체인

VI. GDPR 개인정보 사용 동의 예시

- 유럽 연합 일반 개인정보 보호법 General Data Protection Regulation
- 2018년 5월 25일부터 적용
- EU 거주자의 개인 정보 보호를 강화하고 표준하기 위해 제정
- EU 회원국 국민을 대상으로 정보이용의 투명성을 제공하고 개인정보의 이용을 제한하거나 전부 삭제하도록 요구할 수 있는 권리를 국민에게 부여

적용범위

- EU 내 사업장을 운영하며 개인정보를 다루는 기업(컨트롤러/프로세서)
- EU 외에서 EU거주자에게 재화나 서비스를 제공하는 기업
- EU 거주자의 개인 정보 및 웹 데이터(GPS, IP주소, 쿠키 데이터 등)를 모니터링 하는 기업
- 법인회사가 아닌 실질적으로 활동하는 파견인 경우에도 해당

적용범위의 예시

퍼블리싱 대행사를 통해 유럽에 서비스하는 모바일 게임개발 업체가 유지보수를 위해서 게임개발 업체 직원이 DB 서버에 접근하는 경우에는 GDPR의 적용대상인가?

계약 내용에 따라 다르지만 개인정보 사용과 처리방법을 각 사가 규율하는 내용으로 담겨있으면 컨트롤러로 직접적인 GDPR의 대상이 된다. 리스크를 갖지 않기 위해 게임만 제공하고 모든것은 퍼블리싱 업체가 처리하여 수익만 배분한다고 계약에 명시되어 있다면 대상이 되지 않을 수 있으나 DB서버에 접근할 수 있다면 개인정보 처리가 발생하기 때문에 GDPR의 적용대상이 된다.

EU거주자가 국내 항공사에 탑승하는 경우 탑승객 개인정보를 국내에 보관할 경우

EU거주자의 개인정보를 받아 한국에서 처리하기 때문에 개별 항공사별로 명시적 동의를 받을 필요가 있다. 현지에 서버를 두고 국내에서 조회를 할 경우에도 마찬가지로 정보의 국외 이전으로 보여지기때문에 회사 차원에서 표준계약을 하거나 정보 처리의 적정성 검사를 받거나 정보 주체로부터 명백한 동의를 받아야 한다.

적용범위의 예시

국내의 서비스(주민세 관리 시스템)이 EU국적의 외국인에게 서비스 할 경우에는 적용대상인가?

EU 국적을 소지한 A씨가 국내 거주 당시 주민세를 체납하여 현재 프랑스 파리에 거주할 경우 거주했던 시 지자체에서 독촉장을 파리의 A씨의 주소로 보내려고 할 때 GDPR의 적용대상이 될 수 있을까?

데이터 컨트롤러에 해당하는 지자체가 A씨의 주소를 국내에 거주하는 동안에 취득하였거나 국내의 외국 정부기관(대사관)으로부터 취득하였을 경우 우선 컨트롤러의 거점이 EU에 없으므로 3조 1항에 해당하지 않으며 해당 시스템이 EU내 거주자를 대상으로 서비스를 제공하는 시스템으로 보여지기 어렵기 때문에 역시 3조 2항(a)에 해당하지 않는다. 또한 A씨의 주소취득은 EU내 데이터 주체의 행위를 모니터링하여 취득한 것으로는 보여지기 어렵기 때문에 마찬가지로 3조 2항(b)에도 해당하지 않으므로 컨트롤러인 지자체는 GDPR 적용대상이 아니다.

(하지만 시스템을 구축하고 개인 데이터 처리에 관여하는 데이터 프로세서의 경우에는 적용 대상이 될 수 있음)

Controller & Processor

컨트롤러	프로세서
개인정보 처리의 목적, 성격 범위 및 수단을 결정하는 자연인 혹은 법인	개인정보를 컨트롤러에게 적절한 방법으로 위임받아 처리하는 주체
개인정보 처리 원칙을 준수 하는것을 증명해야 함	컨트롤러를 대신하여 개인정보를 처리하는 스마트 컨트랙트의 개발자는 프로세서에 해당됨
구속력있는 서면에 의한 프로세서 지정 및 의무부과	프로세서는 GDPR 준수여부를 입증하기 위한 모든 정보를 컨트롤러에게 제공할 의무가 있음
규모에 따라 개인정보보안책임자 혹은 역내 대리인 지정 필요	

기업의 개인정보보안 책임강화를 위한 조치사항

- DPO의 지정

인정보의 처리가 공공기관이나 단체에 의해 수행되는 경우, 정보 주체에 대한 정기적이고 체계적인 모니터링이 필요한경우 건강 및 범죄경력 등 민감정보에 대한 대규모의 처리가 필요한경우

- 역내대리인 지정

EU 외에서 개인정보를 대규모로 처리하거나 민감정보 처리 시 EU 역 내에 반드시 대리인을 지정해야 함

정보주체의 동의를 받아야 함

- 진술 또는 적극적 행동을 통하여 자신의 개인정보 처리에 대한 긍정적 의사를 표현하는 것
- 이용약관과 반드시 분리되어야 한다
- 동의가 있었음을 반드시 문서화 할 것
- 만 16세 미만의 경우 친권자의 동의를 얻어야 한다
- 복수목적의 경우 개별적인 동의를 얻어야 한다

Controller의 의무

- 피고용인 250명 이상인 기업의 경우 GDPR준수를 입증하기 위해 개인정보 처리활동의 기록을 문서화 할 의무가 있다
- 피고용인 250명 이하여도 정보주체의 권리를 침해할 경우, 민감정보 처리, 유죄판결 및 형사범죄에 관련된 개인정보 처리 시 처리 활동을 기록해야 한다
- 개인정보 침해 사전신고 및 통지 기업은 GDPR에 따라 정보 주체에게 통지할 필요가 있는 개인정보 침해 유형을 파악하고 72시간 내로 감독 기구에 신고해야 한다

GDPR에서 규정하는 개인정보

- 기본 신상정보(이름, 주소, ID)
- 웹 정보 (위치, IP, 쿠키 데이터, RFID)
- 인종 또는 민족정보
- 정치적 견해
- 성적 취향
- 유전자 및 바이오 인식정보

물적 적용 범위

- 개인정보가 자동화된 수단에 의해 처리된 것
- 수기처리와 같은 개인정보여도 파일링 시스템에 포함되면 해당
- 익명정보에는 적용되지 않으나 가명 정보에는 적용됨
  (식별 가능성으로 분류)

GDPR을 위반할 경우

- 전 세계 매출의 4% 혹은 2000만 유로중 높은 금액을 벌금으로 부과
- 벌금 외 민사소송

블록체인과 상충되는 점

- 블록체인은 트랜잭션 이력을 기록하는 영구 기록물이므로 블록체인의 불가변성은 삭제 및 접근 권한 제한 등의 정보 주체의 권리를 침해한다
- 누구에게나 공개된 원장 (퍼블릭 블록체인)의 투명성은 정보 보안의 규정에 어긋난다

GDPR을 고려한 기업의 블록체인 배치 방법

- 퍼블릭 블록체인 배제
  개인 식별 정보 및 데이터 도메인 관리를 위해 기업은 블록체인의 활용을 온전히 비공개로 하거나 승인을 받는 용도로 쓸 수 있음

- 개인식별정보 관리 블록체인 배제
  개인식별정보 기록 자체가 아닌 기록의 해시값을 블록체인에 등록
  삭제할 해시값은 영구 스토리지에 보관되지만 영구적으로 누구도 접근하지 못하는 방법으로 관리

- GDPR을 준수하는 보안 솔루션의 이용
  기업 내 데이터 스토리지가 아닌 검증 시스템을 구축
  peermount, Fortinet, GDPR Edge 등

보안 솔루션의 예시

- **Peermountain**
  자체 주권 신분 소유자(개인)와 규제 준수 서비스의 제공자(기업)을 연결해주는 분산된 P2P 신탁 서비스

  기업은 고객의 정보가 담긴 Peermountain의 블록체인에서 서비스를 제공하기 위해 얻어야 할 고객정보를 제공받음으로서 기업은 실제 고객의 개인정보를 취급하는데의 비용을 절감하고 위험부담을 줄일 수 있다.

- **Fortinet**
  보안 패브릭 형태를 구성하여 허가받지 않은 노드들의 개인정보 접근을 제한함

  정보주체권리의 침해 혹은 보안 위반 시 보안 패브릭을 통해서 72시간내에 보고될 수 있도록 함

- GDPR Edge
  Intel, Microsoft 등의 회사가 협업하여 개발한 Hyperledger Sawtooth 분산원장 기술을 활용한 솔루션

  개인 식별정보가 담긴 중앙집중식 리포지토리에서 서로 다른 트랜잭션 데이터를 확인하고 동시에 소비자를 위한 외부 동의 메커니즘을 제공함

기업의 준비사항

- **GDPR 적용 대상 여부 판단 및 정보에 대한 이해**
  특히 민감정보(건강, 유전자, 범죄) 또는 아동의 개인정보를
  처리해야 하는 경우 더욱 강화된 기준을 적용받을 수 있으므로 주의
  (사망진단서, 피상속인이 미성년자일 경우)

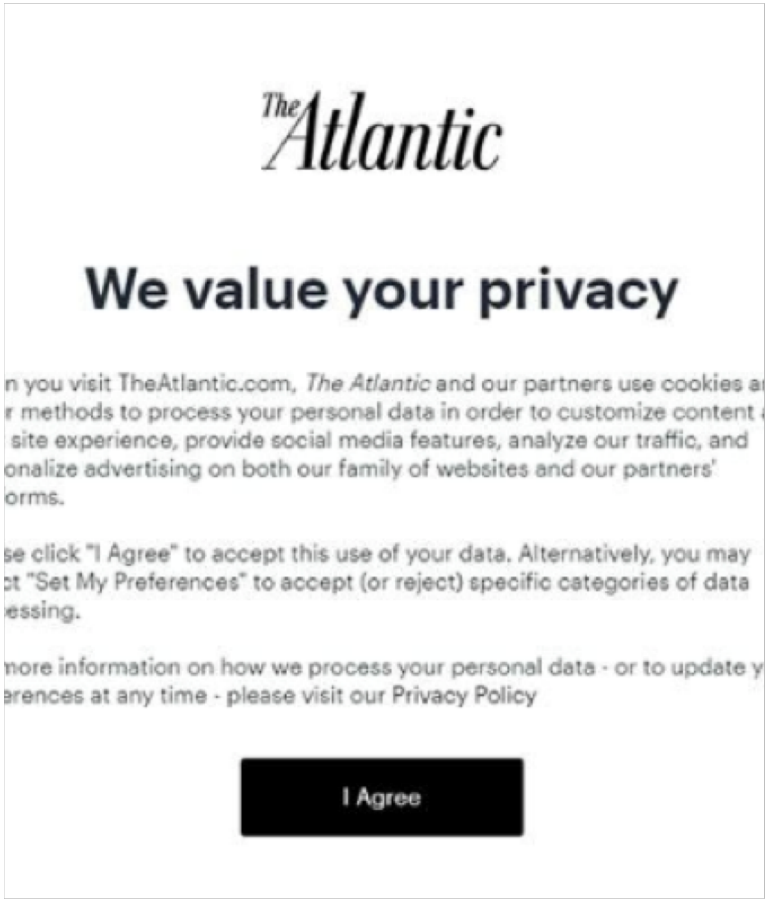
- **데이터 보호 계획 수립**
  개인 정보 데이터가 GDPR의 요구사항과 일치하는지, 일치하지
  않을 경우 개정해야 한다 (데이터 등록의 최소화 및 처리되는 목적 고려)
  동의 절차를 점검하고 GDPR 기준에 맞게 보완

- **사고 대응 계획 수립 및 개인정보 유출 통지 절차 마련**
  데이터 침해 사고 발생 시 72시간내로 보고해야 할 의무가 있기 때문에 규정된 시간 내로 적
  절히 보고 및 대응 할 수 있어야 한다 또한 하나이상의 EU국가에서 활동할경우 어느 국가의
  감독기구의
  관할인지 확인 필요

- **지속적인 평가 프로세스의 준비**
  DPO 임명 및 개인정보 영향평가를 수행하고 영향 평가에 따른 업무 수행을 모니터링

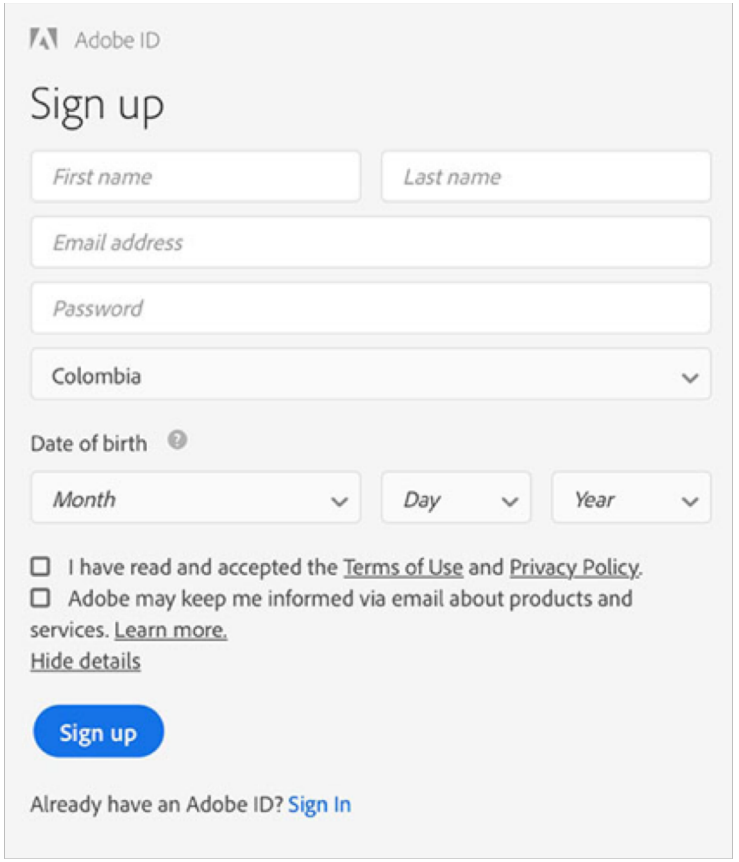
GDPR 개인정보 사용 동의 예시

개인 정보 이용 정책에 변경된 점이 생겼을 경우 사용자가 사이트를 처음 접속할 때 동의를 얻을 수 있도록 한다.



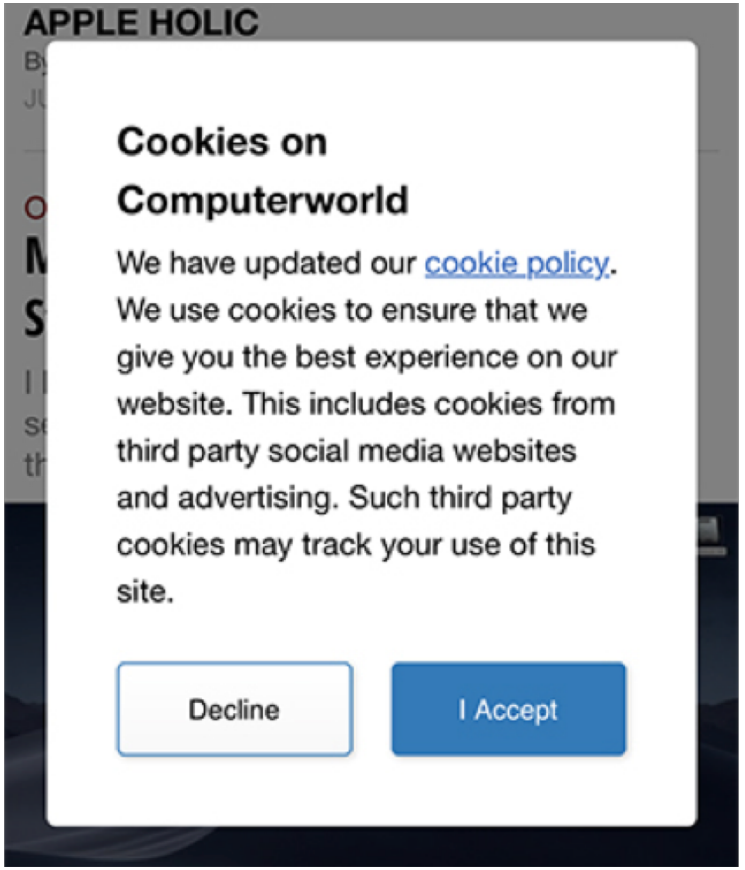
GDPR 개인정보 사용 동의 예시

- 사용자가 법적 계약에 동의하는 부분에 있어 별도로 체크할 수 있어야 한다.
- 사용자가 링크를 통해 정책과 계약에 쉽게 접근 할 수 있도록 한다.
- 체크박스는 사전에 체크가 되어 있어서는 안된다.



GDPR 개인정보 사용 동의 예시

- 쿠키 데이터를 통해 개인을 식별할 필요가 있는 서비스에서는 반드시 정보 이용에 대한 동의를 받아야 함
- 사용자에게 수락 또는 거절 옵션을 명확하게 제공해야 한다.



GDPR 개인정보 사용 동의 예시

사용자가 개인정보 취급과 관련한 사항에 대해 언제든지 문의할 수 있도록 개인 정보 보호 관련 부서의 주소 및 연락처를 게시한다.

Contact Us

If you have any questions, email us at privacy@nytimes.com or write us at:

The New York Times Company

620 Eighth Avenue

New York, NY 10018

Attn.: Privacy Counsel

We can also be reached by phone at 1-800-NYTIMES (click here for a list of our local telephone numbers outside the USA).

For information on how this Privacy Policy applies to your use of NYT Services, please visit the relevant section below.

Reference

•언론
"우리 기업도 GDPR의 적용대상이 되나요?"
http://www.ddaily.co.kr/news/article.html?no=163555
'블록체인과 GDPR' 상극일까, 공생 관계일까?
http://www.itworld.co.kr/news/109231
GDPR, 기업 블록체인 데이터베이스에 된서리 될까
http://www.itworld.co.kr/news/109143

•블로그 및 웹페이지
한국 인터넷 진흥원 GDPR 안내
https://www.kisa.or.kr/business/gdpr/gdpr_tab1.jsp
유럽 이슈 GDPR과 블록체인의 연관성
https://steemit.com/gdpr/@tksehd23/gdpr-general-data-protection-requirement
국내의 주민세 관리 시스템이 GDPR 적용대상이 되는가?
https://blog.naver.com/misman95/221251000667
•Blockchain & GDPR (프랑스 CNIL 보고서)
https://sooyongshin.wordpress.com/2018/12/11/blockchain-gdpr-%ED%94%84%EB%9E%91%EC%8A%A4-cnil-%EB%B3%B4%EA%B3%A0%EC%84%9C/
GDPR Consent Examples
https://termsfeed.com/blog/gdpr-consent-examples/

•Youtube
유럽 연합 GDPR의 이해와 대응방안
https://www.youtube.com/watch?v=4G-FpJBz3cw&t=2831s

contact@returnvalues.com