공공서비스에서의 개인정보보호중심 설계

제3회 서울시 개인정보보호 포럼

-디지털플랫폼 구축의 처음과 끝, “개인정보”-

2022. 6. 3. 13:00-17:00

코엑스 그랜드볼루

김보라미

법률사무소 디케 변호사

squ24n@gmail.com

생각해보기


Tag Your Friends
This will quickly label your photos and notify the friends you tag. Learn more
Who is this?
Who is this?
Who is this?
Who is this?
Who is this?
Who is this?
Francis Luu


MBC NEWS
단돈 2만원에‥'보복 살인' 이석준
범행 정보원은 '구청 공무원'

목표

- 개인정보보호 중심설계는 무엇인가.
- 개인정보보호 중심설계는 왜 중요한가.
- 공공서비스에서 개인정보보호 중심설계를 위한 검토

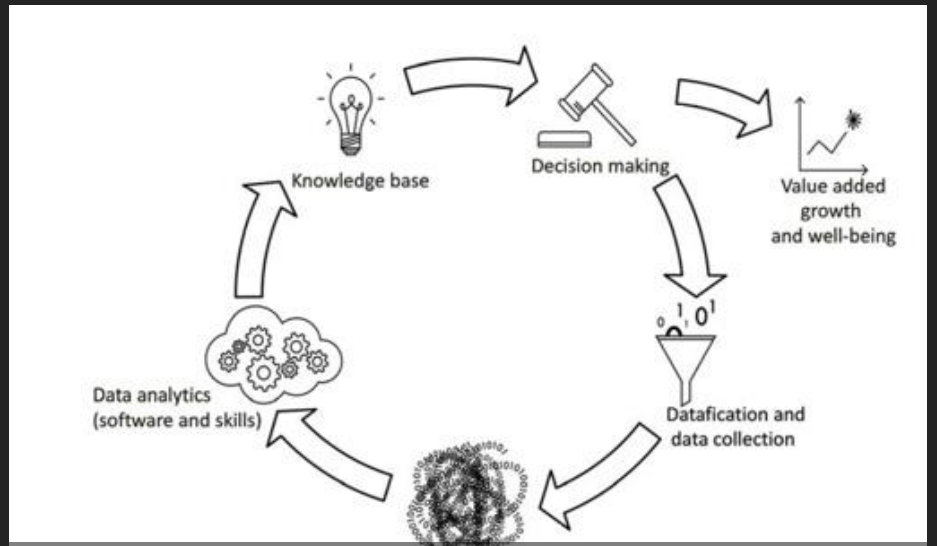
디지털 시대의 신기술

신기술이란,

가상적, 물리적, 그리고 생물학적 영역간 경계를 전환하는 기술의 혁신으로 ① 데이터로의 전환, ② 데이터 배포, ③ 자동화된 의사결정을 위한 기술들을 포함

신기술과 인간의 삶

- 복합적인 과정
- 오프라인과 온라인의 동기화(Physical-Digital-Physical loop) : 데이터화(탈육체화) - 디지털정보의 배포 및 이전 - 의사결정
- 상호연관적으로 인간의 삶에의 작용



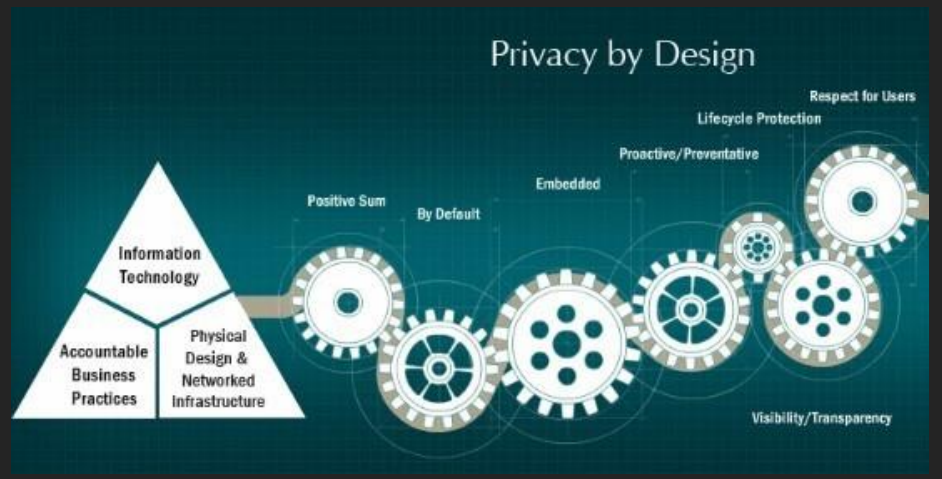
<출처 : https://tomvanwoensel.com/the-transport-analytics-lab/>

일상의 사물 위협

- <https://slate.com/technology/2015/08/twitter-account-internet-of-shit-mocks-ridiculous-internet-of-things-technologies.

개인정보보호 중심설계

- 출처 http://privacybydesign.ca



개인정보보호 중 심설계의 7대 원칙

1. 사후대응이 아닌사전대비
2. 프라이버시 보호를 기본 설정(default setting)
3. 전체 수명주기 보호
4. 완전한 기능성 보장 – 제로섬이 아니라 포지티브 섬
5. 가시성과 투명성
6. 개인의 프라이버시 존중 – 이용자중심
7. 기획단계에서 고려

유럽 개인정보보호법 제25조 설계 및 기본설정에 의한 개인정보보호

◆ 유럽개인정보보호법

- 2016년 4월 14일 유럽의회에서 의결되어 2018년 5월 25일 시행
- 프로파일링 시대에 개인정보처리 원칙과 개인정보주체의 권리, 보호조치 등을 과거 지침(directive)에서 보다 구체화
- 위반시 경우에 따라 최대 20,000,000유로 또는 직전 회계연도의 연간 전 세계 총 매출의 4%에 이르는 행정 과징금 중 높은 금액의 처분을 받게 하는 등 행정과징금의 액수도 상향 조정

- 1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

- 2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

- 3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

유럽 개인정보보호법 상 개인정보보호 중심설계 의무

전문 (78) 개인정보의 처리와 관련하여 자연인의 권리와 자유를 보호하기 위해서는 적절한 기술적·관리적 조치를 시행함으로써 본 규정의 요건을 충족시켜야 한다. 본 규정의 준수를 입증하기 위해 컨트롤러는 특히 개인정보보호 최적화 설계 및 기본설정의 원칙을 충족시키는 내부 정책과 조치를 채택하고 시행하여야 한다. 그 같은 조치는 무엇보다 개인정보 처리의 최소화, 가능한 빠른 시일 내 적용되는 개인정보의 가명처리, 개인정보의 기능 및 처리에 관한 투명성으로 구성되고, 이를 통해 정보주체는 정보처리를 모니터링하고 컨트롤러는 보안을 확립 및 개선할 수 있다. 개인정보의 처리를 기반으로 하거나 작동 중에 개인정보를 처리하게 되는 애플리케이션·서비스·제품을 개발, 설계, 선택, 활용할 시, 해당 제품·서비스·애플리케이션의 생산자는 이를 개발하고 설계할 때 개인정보 보호 권리를 고려하고 최첨단 여부를 적절히 살펴 컨트롤러와 프로세서가 개인정보보호의 의무를 준수할 수 있도록 보장해야 한다*. 개인정보보호 최적화 설계 및 기본설정의 원칙은 공개입찰 시에도 고려되어야 한다.*

- 최소처리원칙의 현대적 실현

제25조 설계 및 기본설정에 의한 개인정보보호

1. 컨트롤러는 개인정보의 처리가 자연인의 권리 및 자유에 미치는 위험의 다양한 가능성 및 정도와 함께 최신 기술, 실행비용, 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 기술 및 관리적 조치는 본 규정의 요건을 충족시키고 개인정보주체의 권리를 보호하기 위해 **데이터 최소화 등 개인정보보호 원칙을 효율적으로 이행하고 필요한 안전조치를 개인정보처리에 통합할 수 있도록 설계되어야 한다.**

2. 컨트롤러는 기본설정을 **통해 각 특정 처리 목적에 필요한 개인정보만 처리되도록 적절한 기술 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

유럽연합 PbD 가이드라인상 9가지 구현원칙 (2020. 10. 20. 개정)

1. **투명성** -정보주체가 자신의 권리를 이해하고 이를 행사할 수 있는 정보를 제공하는 것을 포함
2. **적법성** – 개인정보 처리의 법적 근거에 그 처리가 부합해야 한다는 원칙
3. **공정성** -개인정보가 부당하게 차별적이거나, 예상할 수 없거나, 오해의 소지가 있는 방법으로 처리되지 않아야 한다는 원칙
4. **목적제한성**- 특정되고 명시적이며 합법적인 목적으로 데이터를 수집해야 한다는 원칙
5. **데이터 최소성** - 적절하고 관련성이 높으며 목적에 필요한 것으로 제한된 개인정보만 처리할 수 있는 원칙
6. **정확성** – 개인정보가 정확하고 최신 상태로 유지되어야 하며, 처리 목적과 관련하여 부정확한 개인정보가 지체 없이 삭제 되거나 수정되도록 보장하기 위해 모든 합리적인 조치가 취해져야 한다는 원칙
7. **스토리지 제한성** - 개인정보가 특정 목적을 위해 필요한 기간동안만 보관하다록 제한하는 원칙
8. **무결성과 기밀성** - 개인정보에 대한 기술적 또는 조직적 조치를 활용한 침해사고 예방, 관리 등의 원칙

개인정보보호 중심 설계의 고려

개인정보가 불특정 다수에게 열람되지 않는 것을 포함한 기본설정을 통해/ 처리 목적에 필요한/ 최소한의 개인정보만 처리되도록/ 기술적·관리적 조치의 도입

개인정보보호 중심 설계기준과 기본설정준수기준 마련

1. 이용자들의 권리에 미치는 위험성
2. 개인정보 침해적 기술의 도입 여부
3. 비용
4. 개인정보처리의 성격, 범위, 맥락 및 그 목적
5. 개인정보보호 원칙

공공서비스와
민간서비스의 만남

서비스 설계와 디자인에 대한 의문

프라이버시 중심 디자인은 어떻게 하는가? – 우드로 하초그(에이콘, 2021)

1. 감시 기술은 탐지될 수 없도록 디자인돼야 할까?
2. 이용자들의 개인정보를 공유하기 위해 어떤 기술적 보안 기술을 적용해야 할까?
3. 제3자 제공, 공유를 부추기는 기능, 기본 설정, 그리고 구조적 문제는 없는가
4. 소프트웨어 인터페이스의 한계는 없을까?
5. 일상의 사물과 인터넷을 연결할 때 어떤 정책을 가져야 하는가

고맙습니다.