



**THREE ESSENTIAL THOUGHTS
ON DESIGNING PRIVACY INTO YOUR BUSINESS**

Information session at Helsinki Think Company / 18.4.2017



- 1) PRIVACY BASICS**
- 2) PRIVACY BY DESIGN**
- 3) OPERATING WITH PRIVACY**



PRIVACY BASICS:

RELEVANT LAW: FINNISH PERSONAL DATA ACT



- The Act regulates processing of personal data.
- The Act defines personal data as any information on a private individual and any information on his/her personal characteristics or personal circumstances, where these are identifiable as concerning him/her or the members of his/her family or household



EXAMPLES OF PERSONAL DATA

- Your name
- Telephone number
- Home address
- Credit card details
- Health information
- Personal identity code
- Email address
- Password(s), etc



PROCESSING OF DATA

- Processing of personal data means the collection, recording, organisation, use, transfer, disclosure, storage, manipulation, combination, protection, deletion and erasure of personal data, as well as other measures directed at personal data;



OTHER KEY TERMS

- Controller:

A person, corporation, institution or foundation, or a number of them, for the use of whom a personal data file is set up and who is entitled to determine the use of the file, or who has been designated as a controller by an Act

- Data subject:

A person to whom the personal data pertains.



- Third party:

A person, corporation, institution or foundation other than the data subject, the controller, the processor of personal data or someone processing personal data on the behalf of the controller or the processor



APPLICATION OF THE FINNISH PERSONAL DATA ACT

- (1) The Act applies to processing of personal data where the controller is established in the territory of Finland or otherwise subject to Finnish law.
- (2) The Act also applies if the controller is not established in the territory of a Member State of the European Union but uses equipment located in Finland in the processing of personal data.
- An exception is where the equipment is used solely for the transfer of data through the territory in which case the controller shall designate a representative established in Finland.



REGULATION (EU) 2016/679

- The protection of natural persons with regard to the processing of personal data and on the free movement of such data
- The regulation aims to harmonize the level of protection in all member states of the European Union.
- The regulation shall apply from 25 May 2018.



PRIVACY BY DESIGN

privacy protection becoming more 'design-driven'




WHAT IS PBD?

- The realisation of privacy values in the physical/digital design of the end product or service
- = technology and design-based solutions coming to the heart of bolstering privacy laws



DESIGN ≠ AESTHETICS



**DESIGN = UTILITY AND
FUNCTIONALITY**



- **PBD is shifting the burden** to implement privacy laws from data controllers to the manufacturers and developers of the technology concerned



WHICH IS MORE EFFECTIVE?

- Rules regulating behaviour
- OR
- code/physical architecture regulating behaviour



DESIGN PROCESS

1. Privacy legislation
2. Privacy risk assessment of your business
3. Realisation of a design solution minimising the privacy-intrusive capabilities of your business



LEGAL RELEVANCE OF PBD

- Check Article 25 of **REGULATION (EU) 2016/679**
- --> PBD legally required from anyone processing personal data!
- --> is a glued-on privacy policy sufficient after the implementation of the GDPR?



HOW DOES PBD BENEFIT YOUR STARTUP?

- More effective ensuring of compliance
- Minimisation of privacy-intrusive measures
- Unique selling point
- Source of value creation
- Enhances trust



OPERATING WITH PRIVACY



SO, YOU'RE UP AND RUNNING...



NOT QUITE THAT EASY...

- .. shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
 - (a) the pseudonymisation and encryption of personal data;
 - (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
 - (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
 - (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.



ALONG COMES AN IDEA: CAN I DO X WITH THE DATA?

X = Something you did not
specify originally in your
privacy policy



NOT QUITE THAT EASY...

- Is the new purpose compatible with the original?
- If in doubt, ask the Data Protection Ombudsman (<http://www.tietosuoja.fi/fi/>)
- If still unsure, ask for consent



WHAT DO YOU DO WHEN THERE'S A BREACH?

1. Stay calm !
2.
 - **Contain** → stop further leaks
 - **Notify**
 - the authorities, always (72 h)
 - the data subjects, possibly
 - **Recover** → has the data been altered?
 - **Fortify** → stop from happening again