Data Protection

For Developers from a Company's View

What's your experience?

- Implemented data protection management?
- Any touch points in your work?
- Happy? Annoyed?

GDPR

- Since 25.5.2018
- Applies for all companies processing data of EU-citizen
- Applies directly for all countries, without them having it to implement it in national law
- Lex Generalis - general regulation, a lex specialis can give more regulations for special fields (E-Privacy, TKG, ...)
- Huge fines (...at least in theory: http://www.enforcementtracker.com/)
- Still no clear answers to all questions
- Other countries follow (with aim to have adequacy):
    - USA (at least California)
    - Japan
    - Brasil

Definitions

1) Data Classification (https://gdpr.niobase.app/en/article/4, https://gdpr.niobase.app/en/article/9,

   https://gdpr.niobase.app/en/article/10)
   a) Personal Data
   b) Special Categories (Ethnic, Political, Religion, Genetics, Biometric, Health)
   c) Data Relating to Criminal Offences
2) Main Roles: (https://gdpr.niobase.app/en/article/4)
   a) Controller
   b) Processor
   c) Data Subject

Definitions

3) Principles relating to processing of personal data ()
   a) Lawfulness
   b) Purpose binding
   c) Data Minimisation
   d) Accuracy
   e) Storage Limitation
   f) Integrity and confidentiality

What to do? - Document Processing Activities

1) Discover Processes where personal data is processed
   a) Also pseudo-anonymized, but not anonymized
2) Set purpose
3) Find Legal Basis (https://gdpr.niobase.app/en/article/6)
   a) Consent
   b) Contract
   c) Legal Obligation
   d) Vital Interest
   e) Public Interest
   f) Legitimate Interest
4) Define retention and storage period
5) Self assess risk of processing
6) Document measures to ensure safe processing

What to do? - Prepare for Data Subject Requests

- Right of access by the data subject (https://gdpr.niobase.app/en/article/15)
- Right to recitification (https://gdpr.niobase.app/en/article/16)
- Right to erasure ('right to be forgotten') (https://gdpr.niobase.app/en/article/17)
- Right to restriction of processing (https://gdpr.niobase.app/en/article/18)
- Right to data portability (https://gdpr.niobase.app/en/article/20)

What to do? - Prepare for Data Breaches

- 72h to report to data protection authorities (https://gdpr.niobase.app/en/article/33)
- Communication of a personal data breach to the data subject (https://gdpr.niobase.app/en/article/34)

What to do? - Inform and get Consent

- Inform user before processing what data you process for what purposes
- Decision from EuGH for Opt-In Cookies for non technical cookies

  (https://www.golem.de/news/eugh-urteil-jeder-cookie-erfordert-einwilligung-der-nutzer-1910-144187.html)

What's next?

- Continuous improvement
- More definitive decisions
- e-Privacy (~ Q2 - Q4 2020)