Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

Data Protection by Design and by Default in GDPR

Facilitating GDPR compliance for SMEs and promoting Data Protection by Design in ICT products and services (www.bydesign-project.eu)

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

ΚΕΝΤΡΟ ΕΡΕΥΝΩΝ ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΠΕΙΡΑΙΩΣ

ICT abovo Information & Communication Technologies

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Agenda of the Seminar

- Relevant Challenges, Main elements, Importance
- Roles and stakeholders
- Software development with Data Protection by Design and by Default
- DPbD (early) approaches
- By default vs. by design

Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

Data Protection by Design (DPbD)

Art. 25(1) of the GDPR

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

What the GDPR says…

- "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".
- This also has to do with system producers/developers (see Recital 78)

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Relevant Challenges

- A “generic” obligation: No specific measures are implied
  - The chosen measures and safeguards should be specific to the implementation of data protection principles into the particular processing in question
- Decisions should based on:
  - *State of the art*
  - *Cost of implementation*
  - *Nature, scope, context and purpose of processing*
  - *Risks for rights and freedoms*
- *Time aspect*
  - *From the beginning and during the processing*

Implementation of data protection principles (in an effective way)

By Design!!

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Main elements

- Proactive – not reactive
- Embed privacy into the design process
- Not only security aspects!
  - Much broader than “security-by-design”

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Effectiveness - heart of DPbD

- Implement the principles in an “effective manner”
  - implement measures and safeguards to protect data protection principles
  - Each implemented measure should produce the intended results for the processing
  - The measures and safeguards should be designed to be robust and the controller should be able to implement further measures in order to scale to any increase in risk

  - Controllers should be able to **demonstrate that the principles have been maintained**.
  - Documentation of the implemented technical and organizational measures.
    - Appropriate key performance indicators (KPI) to demonstrate the effectiveness.
      - Quantitative, such as the percentage of false positives or false negatives, reduction of complaints, reduction of response time when data subjects exercise their rights; or
      - Qualitative, such as evaluations of performance, use of grading scales, or expert assessments.
    - Alternatively, controllers may be able to demonstrate the effective implementation of the principles by providing the rationale behind their assessment of the effectiveness of the chosen measures and safeguards

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Why is DPbD important?

- If not implemented or implemented incorrectly:
  - "Wrong" decisions on the processing may be taken
    - Yielding issues in terms of (effectively) fulfilling personal data protection principles
  - Mitigating measures may be impossible or with high cost
    - A (total?) re-design may be necessary

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Non only for data controllers…

- Processors and producers - Key enablers for DPbDD
  - Should be aware that controllers are required to only process personal data with systems and technologies that have built-in data protection
  - Should use their expertise to build trust and guide their customers, including SMEs, in designing /procuring solutions that embed data protection into the processing
  - The design of products and services should facilitate controllers' needs
  - Should play an active role in ensuring that the criteria for the "state of the art" are met, and notify controllers of any changes to the "state of the art" that may affect the effectiveness of the measures they have in place.
  - Producers should strive to demonstrate DPbDD in the life-cycle of their development of a processing solution.
  - Controllers, processors and producers, should consider their obligations to provide children under 18 and other vulnerable groups with specific protection in complying with DPbDD

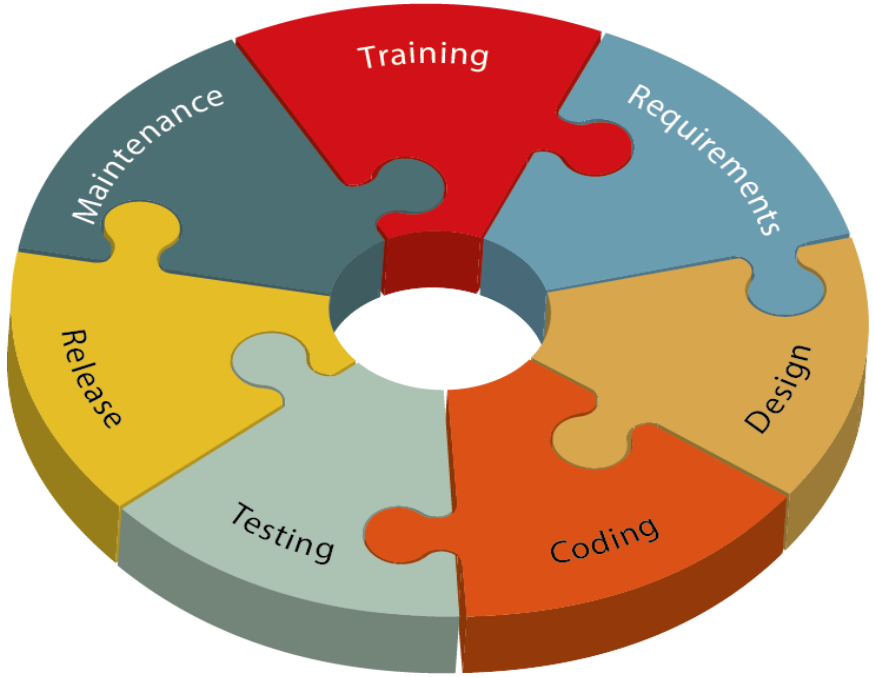
Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Possible stakeholders and roles

- System engineers: In charge of design and development
- Security managers/officers: In charge of network and systems/applications security
- Data Protection Officer: Independent consulting from a data protection point of view
- Project managers: Senior executive in charge of development
- End users: Users of the system performing personal data processing
- Data subjects

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Software development with Data Protection by Design and by Default



https://www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/?print=true

Training: Important data protection topics

Requirements: measures needed to ensure data protection and security, the tolerance levels the organisation should set for data protection and security, and the need to assess both security risks and data protection implications.

Design, data oriented and process oriented design requirements. Threat modelling and an analysis of the attack surfaces.

Coding : use of approved tools and frameworks, disabling unsafe functions and modules, and regularly carrying out static code analysis and code review.

Testing: test whether data protection and security requirements are implemented properly

Release, incident response plan, security review, release approval

Maintenance: prepared to respond to incidents, personal data breaches, faults and attacks, and be capable of issuing updates, guidelines, and information to users and those affected by the software

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Some (early) approaches

- Kung, 2014

Depending on the context/purpose

Strategy		Tactics Examples
1 Minimization	Collection of personal information should be kept to a strict minimum	• Anonymize credentials (e.g. Direct anonymous attestation) • Limit processing perimeter (e.g. client processing, P2P processing)
2 Enforcement	Provide maximum protection of personal data during operation	• Enforce data protection policies (collection, access and usage, collection, retention) • Protect processing (e.g. storage, communication, execution, resources)
3 Transparency and accountability	Maximum transparency provided to stakeholders on the way privacy preservation is ensured	• Log data transaction • Log modifications (policies, crypto, protection) • Protect log data
4 Modifiability	Cope with evolution needs	• Change Policy • Change Crypto Strength and method • Change Protection Strength

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Some (early) approaches

- Hoepman, 2014

Depending on the context/purpose

Strategy		Patterns Examples
1 Minimization	Amount of processed personal data restricted to the minimal amount possible	• select before you collect • anonymisation / pseudonyms
2 Hide	Personal data, and their interrelationships, hidden from plain view	• Storage and transit encryption of data • mix networks • hide traffic patterns • attribute based credentials • anonymisation / pseudonyms
3 Separate	Personal data processed in a distributed fashion, in separate compartments whenever possible	• Splitting data bases (e.g. through pseudonyms)
4 Aggregate	Personal data processed at highest level of aggregation and with least possible detail in which it is (still) useful	• aggregation over time (used in smart metering) • dynamic location granularity (used in location based services) • k-anonymity • differential privacy
5 Inform	Transparency	• Platform for privacy preferences • Layered approach for information (no large texts)
6 Control	Data subjects provided agency over the processing of their personal data	• User centric identity management • End-to-end encryption support control
7 Enforce	Privacy policy compatible with legal requirements to be enforced	• Access control • Sticky policies and privacy rights management
8 Demonstrate	Demonstrate compliance with privacy policy and any applicable legal requirements	• privacy management systems • use of logging and auditing

Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

Data Protection by Default

Art. 25(2) of the GDPR

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Why is data protection by default important?

- When designing IT systems or IT-based services, the default settings, are of vital importance
- Recognizing the role of the default settings, the GDPR introduces a relevant obligation to data controllers: "*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*".

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

By default vs. by design

- The obligation for data protection by default is closely interlinked with the one on data protection by design
- It might be perceived only as a substantiation of data protection by design
- However, the task of selecting and implementing the default settings has its own specific significance and challenges.
  - Choosing the defaults is not trivial, even with security and data protection by design in mind
  - It requires an assessment of the necessity for each purpose of the processing, balanced with other equally important requirements, such as usability and expected behaviour of the system or service

Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

Thank you for your participation!