Funded by European Union's Rights, Equality and Citizenship Programme (REC)

Personal Data Protection

byDesign: Facilitating GDPR compliance for SMEs and promoting Data Protection by Design in ICT products and services

(www.bydesign-project.eu)

Funded by European Union's Rights, Equality and Citizenship Programme (REC)

Relationship between personal data protection and security

- Principles related to personal data processing (Article 5(1) GDPR):
  - "(a) **lawfulness, fairness and transparency**
  - (b) **purpose limitation**
  - (c) **data minimisation**
  - (d**) Accuracy**
  - (e) **Storage limitation**
  - (f) processed in a manner that ensures appropriate *security* of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('**integrity and confidentiality**')."
- Article 5(2) GDPR adds that:
  - "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('**accountability**')."
- Security is present in several other provisions of the GDPR

Funded by European Union's Rights, Equality and Citizenship Programme (REC)

The notion of risk in data protection

- The GDPR adopts a risk-based approach for data protection and security
  - Not a new concept – already known from the current Directive 95/46/EC
  - The Article 29 Working Party already was in favor of the inclusion of a risk-based approach in the EU data protection legal framework.
    - The Working Party recognizes that some of the provisions in the proposed Regulation may pose a burden on some controllers which may be perceived as *unbalanced* and has therefore in earlier opinions already expressed the view that all obligations must be *scalable* to the controller and the processing operations concerned. Compliance should never be a box-ticking exercise, but should really be about ensuring that personal data is *sufficiently* protected. How this is done, may differ per controller..... Data subjects should have the *same level* of protection, regardless of the size of the organisation or the amount of data it processes. Therefore the Working Party feels that all controllers must act in compliance with the law, though this can be done on in a scalable manner." (WP29 statement, 2013)
- There is no question of the rights of individuals being weakened in respect of their personal data
  - Those rights must be just as strong even if the processing in question is relatively 'low risk'. Rather, the scalability of legal obligations based on risk addresses compliance mechanisms. This means that a data controller whose processing is relatively low risk may not have to do as much to comply with its legal obligations as a data controller whose processing is high-risk.

Funded by European Union's Rights, Equality and Citizenship Programme (REC)

The notion of risk in data protection

- Recital 74 of the GDPR states unambiguously that measures of controllers should take into account the risk to the rights and freedoms of natural persons.
- Various provisions in Chapter IV of the GDPR on the obligations of the controller and the processor specifically refer to "risk", "high risk" and risk assessment (including data protection impact assessment).
- Organisations are required to assess the "likelihood and severity of risk" of their personal data processing operations to the fundamental rights and freedoms of individuals.
  - This does not affect the fulfillment of data subjects rights
- Consequently, processing operations which raise lower risks to the fundamental rights and freedoms of individuals may generally result in fewer compliance obligations, whilst "high-risk" processing operations will raise additional compliance obligations, such as data protection impact assessments (DPIAs).
- In effect, this also links to the notion of "scalability" which envisages that the required compliance and accountability measures should take into account the nature, scope, context and purposes of the processing.
  - Scalability and the risk-based approach are closely linked mechanisms incentivising accountability, based on the specificities of a particular processing operation.
- The GDPR requires DPAs to create lists of the kinds of high-risk processing operations requiring a DPIA
- The GDPR also requires the European Data Protection Board ("EDPB") to issue guidelines, recommendations and best practices on data breaches that may result in "high risk" to individuals.

Funded by European Union's Rights, Equality and Citizenship Programme (REC)

The notion of risk in data protection

- The GDPR adopts a coherent risk based approach throughout its provisions
  - in Articles 24, 25, 32, 33, 34 and 35 with a view to identify appropriate technical and organisational measures to protect individuals, their personal data and comply with the requirements of the GDPR.
  - The risk and the assessment criteria are the same: the assets to protect are always the same (the individuals, via the protection of their personal data), against the same risks (to individuals' rights and freedoms), taking into account the same conditions (nature, scope, context and purposes of processing).
- The risk based approach does not exclude the use of baselines, best practices and standards.
  - These might provide a useful toolbox for controllers to tackle similar risks in similar situations (nature, scope, context and purpose of processing).
  - Nevertheless, the obligation in Article 25 (as well as Articles 24, 32 and 35(7)(c) GDPR) to take into account "risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing" remains.
  - Therefore, controllers, although supported by such tools, must always carry out an assessment of data protection risks for the processing activity at hand and verify the effectiveness of the measures and safeguards proposed.

Funded by European Union's Rights, Equality and Citizenship Programme (REC)

Personal Data Protection Risks Vs Security Risks

- Risk Definition (Recital 75)
  - The risks to the rights and freedoms of individuals of "varying likelihood and severity" may result from personal data processing which could lead to "physical, material or non-material damage"
- Non-exhaustive list of examples of such "physical, material or non-material damage" and of processing activities that could result in such damage (Recital 75)
  - Discrimination
  - Identity theft / fraud, financial loss
  - Reputation damage
  - Loss of confidentiality of personal data protected by professional secrecy
  - Unauthorised reversal of pseudonymisation
  - Any other significant economic or social disadvantage
  - Individuals deprived of rights and freedoms, or prevented from exercising control over their data
  - Processing sensitive data, including data on racial or ethnic origin, political opinions, religion or philosophical beliefs, trade-union membership; genetic data; health data; data concerning sex life; or data on criminal convictions and offences or related security measures
  - Profiling (personal aspects are evaluated [e.g. analyse or predict work performance, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements] to create or use personal profiles)
  - Processing children's and vulnerable persons' data
  - Processing large amounts of data affecting large numbers of individuals
- Additional examples of risks (Article 32.2)
  - Accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data

Funded by European Union's Rights, Equality and Citizenship Programme (REC)

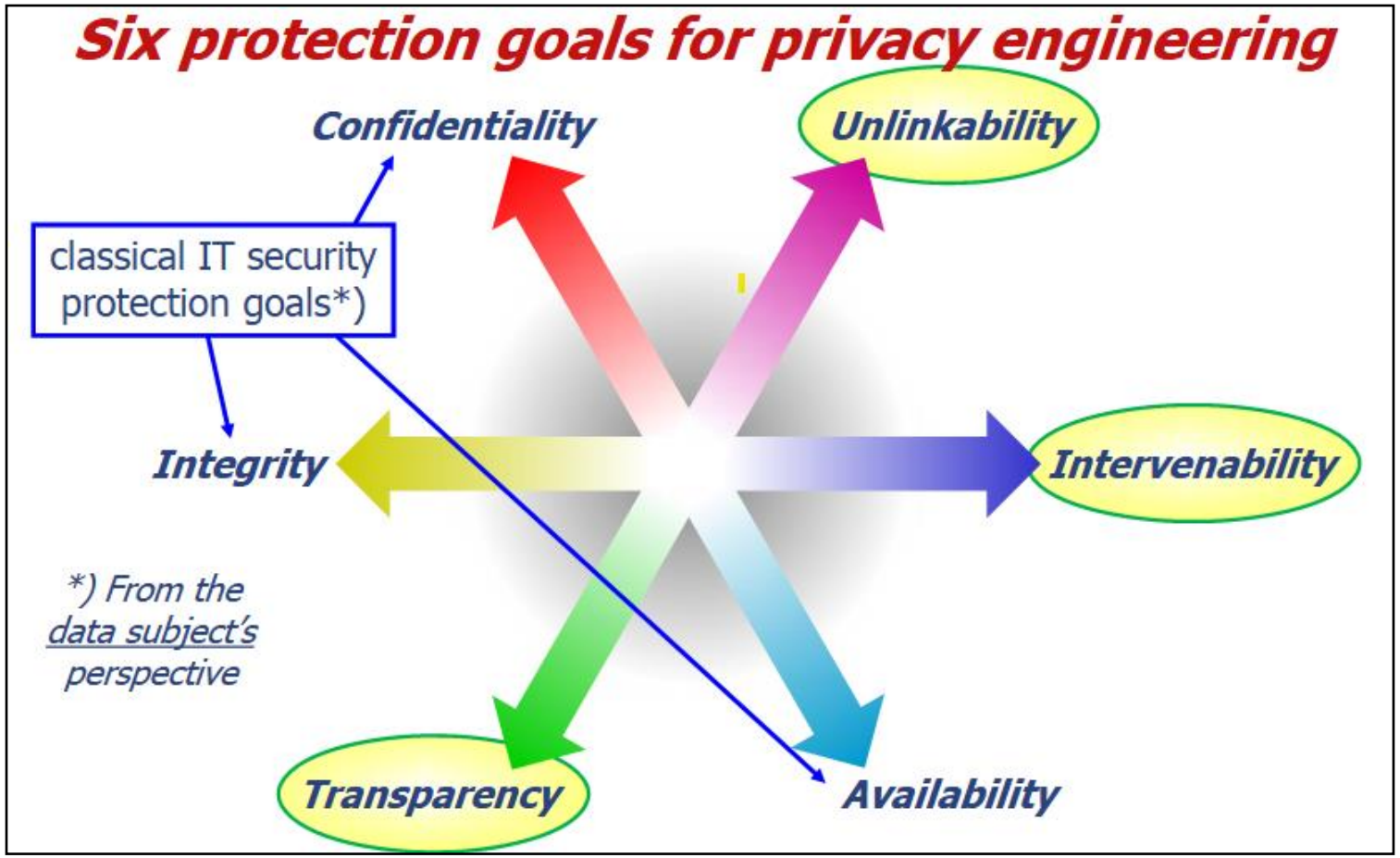
Personal Data Protection Risks Vs Security Risks

- Factors to take into account when determining risk level (i.e. likelihood and severity of risk) (Recital 76)
  - Nature;
  - Scope;
  - Context; and
  - Purposes of processing.
- What types of processing may result in "high risk"?

  Each of the risks above can become "high risk", depending on the "likelihood and severity" of the risks as determined in a risk assessment process by reference to the nature, scope, context and purpose of processing;
  - Processing, "particularly using new technologies", might result in "high risk", depending on "nature, scope, context and purposes of the processing" ("high risk" processing requires an "assessment of the impact" [a DPIA] of the proposed processing operation);
  - New "kind" of personal data processing operation where no DPIA has been conducted or where a DPIA has become necessary over time on the basis of the time elapsed since initial processing; and
  - Large-scale processing operations at regional, national or supranational level and which could affect a large number of data subjects
- Examples of "high risk processing" [Article 35(3)]
  - "Systematic and extensive evaluation of personal aspects ... based on automated processing, including profiling, on which decisions are based that produce legal effects ..."
  - Large-scale processing of sensitive personal data as well as criminal conviction and criminal offence data
  - Large-scale and systematic monitoring of a publicly accessible area.

Funded by European Union's Rights, Equality and Citizenship Programme (REC)

Data protection goals (Transparency, unlinkability, intervenability)



*PROTECTION GOALS FOR PRIVACY ENGINEERING, Marit Hansen, Meiko Jensen, and Martin Rost, International Workshop on Privacy Engineering, 2015

Funded by European Union's Rights, Equality and Citizenship Programme (REC)

Data protection goals (Transparency, unlinkability, intervenability)

- Unlinkability
  - privacy-relevant data cannot be linked across domains that are constituted by a common purpose and context
- Transparency
  - all privacy-relevant data processing – including the legal, technical, and organisational setting – can be understood and reconstructed at any time
- Intervenability
  - intervention is possible concerning all ongoing or planned privacy-relevant data processing.
- Intervenability is not prominent in privacy engineering literature

  Reasons for that:
  - Hard to formalise and to measure
  - Compared with data minimisation research, far less proposed techniques and technologies
  - Can often not be solved within the IT system alone
  - Needs a running system with clear responsibilities (operator, users) – not on prototype level
  - Not one fixed solution, but process-oriented, taking into account the full lifecycle of system evolution

Funded by European Union's Rights, Equality and Citizenship Programme (REC)

Data protection goals: Transparency

- Related to
  - Openness
  - Accountability
  - Documentation
  - Reproducibility
  - Notice (and Choice)
  - Auditability
  - Full-Disclosure
- Implemented by
  - Logging and Reporting
  - User Notifications
  - Documentation
  - Status Dashboards
  - Privacy Policies
  - Transparency Services for Personal Data
  - Data Breach Notifications

See next seminars…

Funded by European Union's Rights, Equality and Citizenship Programme (REC)

Data protection goals: Unlinkability

- Related to
  - Data Minimization
  - Necessity / Need-to-Know
  - Purpose Binding
  - Separation of Power
  - Unobservability
  - Undetectability
- Implemented by
  - Data Avoidance / Reduction
  - Access Control Enforcement
  - Generalization
  - Anonymization/Pseudonymization
  - Abstraction
  - Derivation
  - Separation / Isolation
  - Avoidance of Identifiers

See next seminars…

Funded by European Union's Rights, Equality and Citizenship Programme (REC)

Data protection goals: Intervenability

- Related to
  - Self-determination
  - User Controls
  - Rectification or Erasure of Data
  - (Notice and) Choice
  - Consent Withdrawal
  - Claim Lodging / Dispute Raising
  - Process Interruption
- Implemented by
  - Configuration Menu
  - Help Desks
  - Stop-Button for Processes
  - Break-Glass / Alert Procedures
  - System Snapshots
  - Manual Override of Automated Decisions
  - External Supervisory Authorities (DPAs)

See next seminars…