EU General Data Protection Regulation

Personal data processing security requirements as a result of risk assessment

Georgia Panagopoulou

ICT Auditor at Hellenic Data Protection Authority

gpanagopoulou at dpa.gr

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Accountability and Governance

Data controller responsibility

Objectively demonstrate processing in accordance with GDPR

- Records of processing activities
- Data Protection Impact Assessment (DPIA)
- Privacy by Design, Privacy by Default
- Certifications, Seals, Code of Conduct
- Data Protection Officer (DPO)
- Data Breach Notification

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Security of processing

New in GDPR

- Personal data processors' obligations
- Privacy by Design, Privacy by Default
- Pseudonymization and Encryption
- Confidentiality, integrity, availability and resilience
- Disaster recovery
- Test, assessment and effectiveness evaluation of measures
- Codes of conduct, certifications
- Data breach notifications

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Data Protection Impact Assessment

DPIA = tool to build & demonstrate GDPR compliance

- Obligation if processing "*likely to result in a high risk to the rights and freedoms of natural persons*"
- DPAs define list of the processing operations that require a DPIA
- If high residual risks => consultation with DPA

Risk based approach

Information management system for personal data

Security for privacy

Measures depend on:

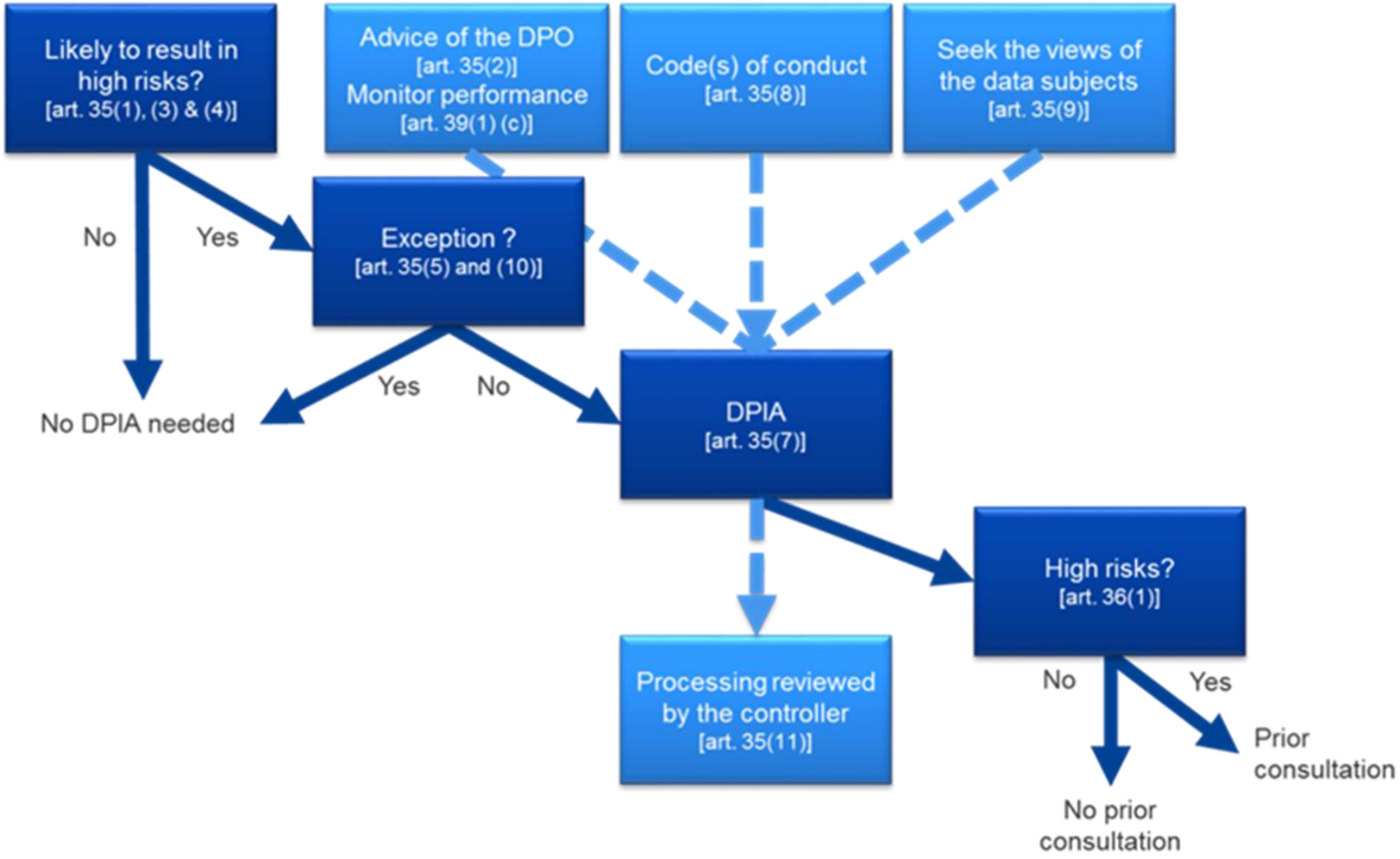
- nature, scope, context, purposes, risks of varying likelihood and severity for rights and freedoms of individuals.

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Data Protection Impact Assessment



Source: WP29

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Data Protection Impact Assessment

Which Processing operations are likely to result in high risk?

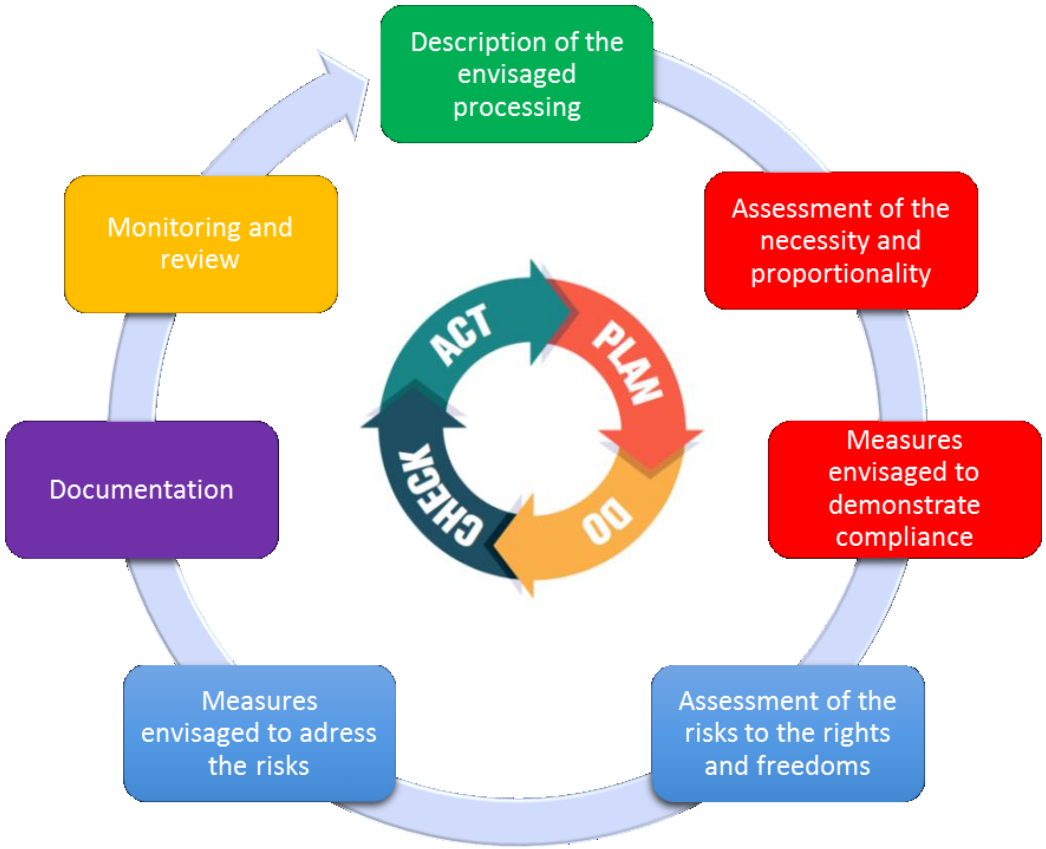
Indicative criteria (WP29 Guidelines)

- Evaluation or scoring
- Automated-decision making with legal or similar significant effect
- Systematic monitoring
- Sensitive data
- Data processed on a large scale
- Data concerning vulnerable data subject
- Innovative use or applying technological or organizational solutions
- Data transfer across borders outside the European Union
- When the processing in *itself "prevents data subjects from exercising a right or using a service or a contract"*

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Data Protection Impact Assessment



Source: WP29

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Data Protection Impact Assessment

Take into account….

Data Protection by Design

- At the time of the determination of the means for processing and at the time of the processing itself . Each new service or business process must take personal data protection into consideration

Data Protection by Default

- Protection of personal data as a default property of systems and services. Activation of safeguards as a default setting

Codes of conduct and certification mechanisms

- Help to specify the measures required, help to demonstrate compliance

Data breach notification obligation

- Data breach staff awareness, internal breach reporting procedure, robust breach detection, investigation and internal reporting procedures

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

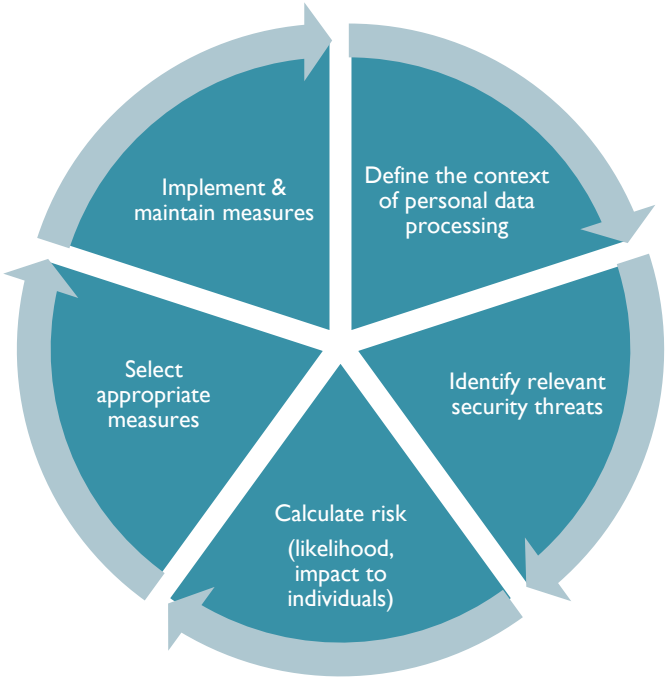
ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Security risk management for personal data

Security risk management for personal data processing ≠ "typical" risk management

- Privacy-specific notion of impact - organization ≠ individuals' freedoms and rights
- Scale may not be relevant
- Secondary adverse effects to be considered
- Different risk acceptance criteria
- Different specific technical and organizational measures
- Multiple security measures of different types (ISO/IEC 27002, ISO/IEC29151…), national standards, supervisory authorities guidelines



Source: ENISA

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Security risk assessment for personal data

Example

Factors to consider for evaluation of impact

- Type of personal data
- Criticality of the processing operation
- Volume of the personal data processed
- Special characteristics of the data controller/processor
- Special characteristics of the data subjects
- Identifiability of the data subjects
- Secondary effects (to the rights and freedoms of individuals)

Assess impact of unauthorized

- disclosure (loss of confidentiality)
- unauthorized alteration (loss of integrity)
- destruction or loss (loss of availability) of personal data

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ
www.dpa.gr

Security risk assessment for personal data

Example: Levels of impact

LEVEL OF IMPACT	DESCRIPTION
Low	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).
Medium	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
High	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc.).
Very high	Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).

Source: ENISA

Security risk assessment for personal data

Define the threats and their likelihood

- Network and technical resources (hardware and software)
- Processes/procedures
- Different parties and people
- Business sector and scale
- Evaluation of threat occurrence probability => Low / Medium / High

		IMPACT LEVEL		
		Low	Medium	High/Very High
Threat Occurrence Probability	Low			
	Medium			
	High			

Source: ENISA

Security risk management for personal data

Example

Organizational security measures

- Security management
- Incident response and business continuity
- Human resources

Technical security measures

- Access control and authentication
- Logging and monitoring
- Security of data at rest
- Network/Communication security
- Back-ups
- Mobile/Portable devices
- Application lifecycle security
- Data deletion/disposal
- Physical security management

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Relevant information sources:

WP 29 - Guidelines http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

- Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679

- CNIL: https://www.cnil.fr/en/privacy-impact-assessments-cnil-publishes-its-pia-manual
- ICO: https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf
- EC - DPIA Template for Smart Grid and Smart Metering Systems: http://ec.europa.eu/energy/en/content/dpia-template-smart-grid-and-smart-metering-systems
- ENISA : Guidelines for SMEs on the security of personal data processing https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Thank you for your attention …

ΑΡΧΗ
ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

www.dpa.gr