EU General Data Protection Regulation

Accountability and Governance Requirements

Georgia Panagopoulou

Privacy and Data Protection Expert - ICT Auditor at Hellenic Data Protection Authority

gpanagopoulou at dpa.gr

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

Records of processing activities

Document personal data protection efforts

Records of processing activities

- Who? (identity of the data controller, the persons in charge of the processing operations and the data processors)
- What? (categories of data processed, sensitive data)
- Why? (purposes of the processing)
- Where? (storage location, data transfers)
- Until when? (data retention period)
- How? (security measures in place)

> 250 employees => internal records of processing operations

< 250 employees => records of higher risk processing operations

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

Content

- Processing operations descriptions, purposes
- Necessity and proportionality assessment
- Assessment of risks to individuals.
- Measures to address risk, including security measures

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

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Data Protection Impact Assessment

Example: Levels of impact

Guidelines for SMEs on the security of personal data processing, ENISA, 2016

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.).

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Data Protection by Design, by Default

Data Protection by Design

Each new service or business process must take personal data protection into consideration

- Data minimization
- Pseudonymization

Data Protection by Default

Protection of personal data as a default property of systems and services

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Certifications, Seals, Codes of Conduct

GDPR endorsement - help to demonstrate compliance

- Codes of conducts and certification mechanisms help specify the measures required
- Certification will be issued by supervisory authorities or accredited certification bodies.
- General criteria for certification, accreditation of certification bodies

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

Data Protection Officer

DPO compulsory

- public authority
- large scale systematic monitoring
- large scale processing of special categories of data or criminal convictions and offences related data

DPO tasks

- advise
- train staff
- conduct internal audits
- monitor compliance
- point of contact for DPAs and individuals

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Data Protection Officer

DPO profile

- reports to the highest mgt level
- independent
- adequate resources
- internal or external
- data protection experience and knowledge

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

Data Breach Notification

Personal data breach definition

- breach of security → destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- more than just losing personal data.

Breach notification obligation to DPA

- within 72 hours
- information in phases
- if needed notification to the public, without undue delay.
- failure to notify breach → fine up to 10 million Euros or 2 % of global turnover

Exc: data encrypted with state of the art algorithm & confidentiality of the key intact → data unintelligible

Notification to individuals

- for high risk

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Data Breach Notification

Breach notification content

- nature of the personal data breach
- categories and number of individuals
- categories and number of personal data records
- name and contact details of the data protection officer
- consequences of the personal data breach
- measures to deal with the personal data breach, mitigate any possible adverse effects

Organization preparation

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

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Role of DPAs

Enforcement, Cooperation and Consistency

- Fines: maximum €20 million or 4% of worldwide turnover.
- Criteria for setting the actual amount
- Cross-border data processing cases→ consultation among affected DPAs to ensure consistency
- Data subjects complaints to the DPA in the MS in which they live or work, or the MS in which infringement occurred.

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Article 29 Data Protection Working Party

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

- Guidelines and FAQ on the right to Data Portability
- Guidelines and FAQs on Data Protection Officers (DPO)
- Guidelines and FAQs on the Lead Supervisory Authority

ΑΡΧΗ
ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

www.dpa.gr

Thank you for your attention …

ΑΡΧΗ
ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ
ΧΑΡΑΚΤΗΡΑ

www.dpa.gr