The byDesign project has received funding from the European Union's Rights, Equality and Citizenship Programme (REC) 2014-2020

"Training material"

Georgia Panagopoulou
ICT Auditor
Hellenic Data Protection Authority

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

(www.bydesign-project.eu)

HELLENIC DATA PROTECTION AUTHORITY

UNIVERSITY OF PIRAEUS RESEARCH CENTER

ICT abovo Information & Communication Technologies

The byDesign project has received funding from the European Union's Rights, Equality and Citizenship Programme (REC) 2014-2020

Training Requirements identified (1/2)

Training in Conceptual Foundation, Practical Examples

1. Data protection/privacy and security risks through DPIA and security risk assessment practical cases/examples.
2. Organizational GDPR roles through practical cases and examples.
3. Data retention periods with industry-specific cases

Training in Privacy by Design Methods, Techniques

4. Data Protection/Privacy by Design requirements in existing ICT services, products, and applications.
5. Data protection/privacy-friendly default configurations for mobile applications.
6. Adjustment of older systems/applications to become privacy friendly.

The byDesign project has received funding from the European Union's Rights, Equality and Citizenship Programme (REC) 2014-2020

Training Requirements identified (2/2)

Training in Privacy Mechanisms	7. Implementation of software tools to preserve personal data protection and to satisfy legitimacy principles
Training in Handling of Data Breaches	8. Mechanisms on data breaches avoidance, monitoring and data breaches handling.
Training in General GDPR Knowledge	9. Guidelines on privacy by design self-assessment

The byDesign project has received funding from the European Union's Rights, Equality and Citizenship Programme (REC) 2014-2020

Training material to meet requirements

1. Data protection/privacy and security risks through DPIA and security risk assessment practical cases/examples.
2. Organizational GDPR roles through practical cases and examples.
3. Data retention periods with industry-specific cases
4. by Design requirements in existing ICT services, products, and applications.
5. By Default configurations for mobile applications.
6. Adjustment of older systems/applications to become privacy friendly.
7. Software tools to preserve personal data protection and to satisfy legitimacy principles
8. Mechanisms on data breaches avoidance, monitoring and handling
9. Privacy by design self-assessment

Security risk assessment vs. data protection risk assessment
ICT organizational GDPR roles – DPIA – examples
Marketing and Advertising, Cookies and trackers

Data Protection by Design and by Default
Data Protection by Design Requirements Elicitation
Data Protection Policies and Notices

Encryption role and techniques
Anonymization role and techniques
Pseudonymization role and techniques

Handling Data Breaches under the GDPR
Measures for preventing / mitigating impacts

The byDesign project has received funding from the European Union's Rights, Equality and Citizenship Programme (REC) 2014-2020

Training material overview (1/5)

1. Introduction to Data Protection Terminology

a. Key GDPR Definitions
b. Data Protection Principles
c. Legal bases
d. Data subjects' rights

2. ICT organizational GDPR roles – DPIA

a. DPO
b. Chief Information Security (CISO)
c. DPO and CISO relationship
d. Privacy team
e. Personal data protection Vs security
f. Risk in data protection
g. Personal Data Protection Risks Vs Security Risks
h. DPIA as GDPR accountability tool and ICT role
i. Role of the DPO with respect to DPIA

The byDesign project has received funding from the European Union's Rights, Equality and Citizenship Programme (REC) 2014-2020

Training material overview (2/5)

3. Security risk assessment vs. data protection risk assessment

a. Information Security Risk Assessment
b. Personal Data Impact Assessment
c. Information Security Risk Assessment vs. Personal Data Impact Assessment
d. Data Protection Impact Assessment Tools and Practical Issues

4. Encryption, Anonymization and Pseudonymization

a. Symmetric encryption
b. Asymmetric encryption
c. Hash functions – MAC – Digital signatures
d. PGP - IP SEC – VPN
e. Anonymization
f. Pseudonymizatio*n*

The byDesign project has received funding from the European Union's Rights, Equality and Citizenship Programme (REC) 2014-2020

Training material overview (3/5)

5. Data Protection by Design and by Default in GDPR

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

6. Implementing the DP principles using DPbyDesign

a. Transparency
b. Lawfulness
c. Fairness
d. Purpose Limitation
e. Data minimisation
f. Accuracy
g. Storage Limitation
h. Integrity and confidentiality
i. Accountability

7. Data Protection Policies and Notices

a. Transparency requirements in GDPR
b. Privacy notices under GDPR – Examples

The byDesign project has received funding from the European Union's Rights, Equality and Citizenship Programme (REC) 2014-2020

Training material overview (4/5)

8. Privacy by Design Requirements Elicitation

a. The Concept of Privacy Requirements
b. Privacy Requirements Elicitation Methodologies
c. LINDUUN, SQUARE for Privacy, PriS, RBAC, STRAP, The i* method, Privacy Requirements Elicitation Technique (PRET), Preparing Industry to Privacy by Design by supporting its Application in Research (PRIPARE), Modelling and Analysis of Privacy-aware Systems (MAPaS Framework), Goal-Based Requirements Analysis Method (GBRAM)
d. Personal Data Retention
e. Data Subjects' Rights Management

The byDesign project has received funding from the European Union's Rights, Equality and Citizenship Programme (REC) 2014-2020

Training material overview (5/5)

9. Handling Data Breaches under the GDPR

a. Definition of GDPR Data Breach
b. Incident handling process
c. Quantifying the risk for data subjects
d. Notification to Supervisory Authority
e. Communication to data subject

10. Attacks causing data breaches, measures for preventing / mitigating impacts

a. Ransomware attacks
b. Data exfiltration attacks
c. Internal human risk source
d. Lost or stolen devices/docs
e. Mispostal
f. Social engineering

11. Online Marketing and Advertising, Cookies, Trackers

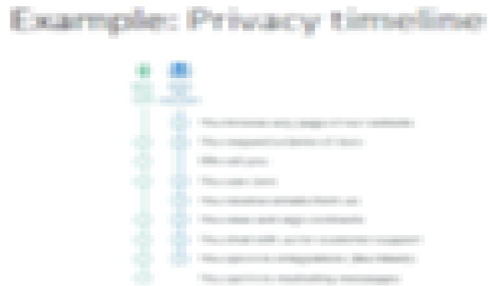
a. e-Privacy Directive - e-Privacy Regulation
b. Direct marketing, e-Marketing
c. Targeted/Behavioral ads
d. Tracking technologies – relevant legislation
e. Cases of cookies - HDPA requirements – examples

The byDesign project has received funding from the European Union's Rights, Equality and Citizenship Programme (REC) 2014-2020

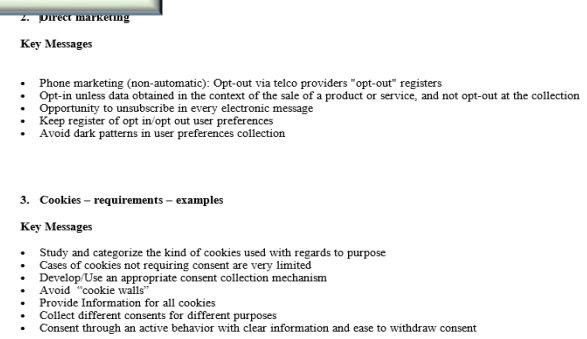
Training material form

Presentation slides

Real world examples, Use cases



Key messages



2. Direct marketing

Key Messages

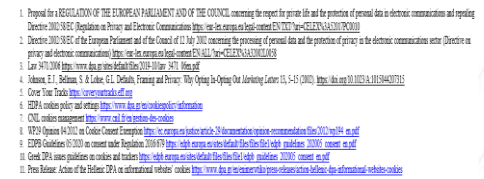
- Phone marketing (non-automatic): Opt-out via telco providers "opt-out" registers
- Opt-in unless data obtained in the context of the sale of a product or service, and not opt-out at the collection
- Opportunity to unsubscribe in every electronic message
- Keep register of opt in/opt out user preferences
- Avoid dark patterns in user preferences collection

3. Cookies – requirements – examples

Key Messages

- Study and categorize the kind of cookies used with regards to purpose
- Cases of cookies not requiring consent are very limited
- Develop/Use an appropriate consent collection mechanism
- Avoid "cookie walls"
- Provide Information for all cookies
- Collect different consents for different purposes
- Consent through an active behavior with clear information and ease to withdraw consent

Lists of references



The byDesign project has received funding from the European Union's Rights, Equality and Citizenship Programme (REC) 2014-2020

Thank you for your participation