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

Handling Data Breaches under the GDPR

byDesign: 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

GDPR – the need for appropriate measures

- **Article 24**: "*1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement* ***appropriate technical and organisational measures*** *to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be* ***reviewed and updated*** *where necessary.*
  2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include ***the implementation of appropriate data protection policies*** *by the controller.*"
- Explicit reference to a General Responsibility of the data controller
- Review and update => Personal Data "legality" Management System (corresponding to an Information security management system - ISMS)
- Provision for appropriate (e.g. individual) data protection policies

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

GDPR and Information Security

- **Article 32**: 1. (…) the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

  (a) the *pseudonymisation* and *encryption* of personal data;

  (b) the ability to ensure the ongoing *confidentiality*, *integrity*, *availability* and *resilience* of processing systems and services;

  (c) the ability to *restore the availability* and access to personal data in a timely manner in the event of a physical or technical incident;

  (d) *a process* for regularly testing, *assessing and evaluating* the effectiveness of technical and organisational measures for ensuring the security of the processing.

- 2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing,(…)

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

What's new?

- ✓Explicit reference to the **obligation of processors** for security measures
- **Proposal** of "appropriate" technical and organizational measures:
  - ➢pseudonymisation and encryption
  - ➢ensure the ongoing confidentiality, integrity, availability and resilience
  - ➢restore the availability and access to personal data in a timely manner
  - ➢a process to test and evaluate security measures
- ✓Use of an approved **code of conduct or certification mechanism** to demonstrate compliance
- ✓**Data protection incident handling procedures**

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

What is a GDPR Data Breach

"…a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"

- The GDPR is applied when information is personal data

Personal Data Breaches ⊂ Security Incidents

Infringement: { **Confidentiality** / **Integrity** / **Availability** } or a combination

GDPR Novelties – Data controller responsibility:

- Recording of all incidents.
- Notification of incidents entailing risk to the Supervisory Authority.
- Informing affected persons about high risk.

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

Incident handling process

Controller **detects**/is made aware of a **security incident** and establishes if personal data beach has occurred.

Controller becomes "**aware**" of a personal data breach and assesses risk to individuals

Risk to individuals' rights and freedoms likely?

NO → No requirement to notify supervisory authority or individuals.

YES → **Notify** competent SA **within 72 h**
In cross-border, notify LSA

High risk likely?

NO → **Καταγραφή** όλων των περιστατικών

YES → **Notify** affected individuals <u>without undue delay.</u>
Information on <u>how to protect themselves</u> from the consequences of the breach.

WP 29
Guidelines on Personal data breach notification under Regulation 2016/679 (wp250rev.01)

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

When does a controller become "aware"?

- There's **no objective definition** of the moment that the controller becomes aware
- Emphasis on **immediate action** to assess whether an incident report is a breach of personal data
  - Investigation time does not "count", as long as the controller's reaction is immediate.
  - One can argue about timing, but is it a good policy?
  - When there's a significant degree of certainty that a beach has occurred => the **72h "timer"** starts.
- **Points of attention** (and control):
  - Internal investigation and handling procedures.
  - Reporting findings to the appropriate persons within the controller.
  - Procedures that are also applied to Processors.
- If the Processor identifies a breach, the Controller should be informed **without undue delay**!
  - 72h start from the moment the Controller is informed, however, processor is responsible
  - Safer stance: an immediate, basic notification, followed by updates.
  - A Processor may notify on behalf of the controller only if this is provided for in their agreement.

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

Providing information to the SA

- a) the nature of the data breach
  - categories and the approximate number of data subjects affected
  - categories and the approximate number of affected files
- b) name and contact details of DPO or other point of direct contact
- c) possible consequences of the breach
- d) measures taken or proposed to be taken by the controller
  - to handle the data breach (the cause of it)
  - to mitigate any adverse effects to data subjects (where appropriate)
- It is also useful to identify any Processors
  - especially since there may be other similar incidents.
- A specific justification of the delay is needed, if exceeding 72 hours.
- **Purpose of the provision**: limiting damage to individuals, by informing them on how to mitigate themselves the consequences of the breach. The Supervisory Authority is informed in order to supervise the actions of the controller
- In complex cases the notification can be done in phases.
  - However, the controller should be able to demonstrate the necessity of partial notification.

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

When notification is not required?

- When the personal data breach is **unlikely** to result in a risk to the rights and freedoms of natural persons
  - While under directive 2002/58/EC all breaches are notified to the SAs

❖When is a personal data breach unlikely to result in a risk?

All 3 parameters of security should be satisfied:

- **Confidentiality**: personal data have been made essentially unintelligible to unauthorised parties
  - Encryption, tokenization
- **Integrity**: Data have not been altered
- **Availability**: Backup is existing and data can be restore within reasonable time

Sometimes the assessment may change over time, due to the state-of-the-art and the risk would have to be re-evaluated

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

Communication to the data subject

- *When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.*
- Obligation to inform only for **high-risk** breaches
  - While every breach entailing risk is notified to the SAs
- **Without undue delay**: The aim is to protect data subjects, so they need to be informed as soon as possible to be able to take measures by themselves
  - **Without undue delay < 72 hours !!!** (ideally)
  - Communication may be delayed if there is a need to address other risks (e.g. to mitigate issues that caused the incident or due to immediate investigation by LEAs)
- Information provided is practically the same as the notification to the SA.
  - Emphasis on recommendations to data subjects on mitigating potential adverse effects

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

Contacting data subject

- Through **individual communication**, for the specific breach
  - Not as part of other information
  - Selection of the medium (s) by maximizing the possibility of receiving the information (email, SMS, Instant messages, banners, mail, media announcements, etc.).
  - Comprehensible and clear, in the language of the data subjects (or at least in the same language as the data collection)
  - See also WP260 - "Guidelines on transparency under Regulation 2016/679"
- Collaborate (informally) with SA for the selection of the appropriate medium

When is direct communication to the subjects not required?

1. When notification to the Authority is not required
   - Unintelligible data, low risk
2. When the controller took action immediately after the incident and a high risk **is no longer likely**
3. When providing individual information requires disproportionate efforts.
   - A public announcement or similar measure is required

- The Supervisory Authority may order the Controller to communicate the breach to the affected data subjects

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

Risk Assessment

- The breach has already occurred, so the focus is wholly about the resulting risk of the impact of the breach on individuals
  - the potential level of impact on individuals
  - how likely is that this risk will materialise

Factors

The type of breach

Confidentiality, Integrity, Availability

The nature, sensitivity, and volume of personal data

Special categories?
Can they be used for identity theft?
Do they reveal information that can pose a threat to a data subject?

Special characteristics of individuals

children or other vulnerable individuals

Severity of consequences for individuals

Identity Theft, Fraud, Discrimination, Physical Dangers, Psychological Stress, Deportation, Reputation Damage, Denial of Critical Service.
What is the relationship between Data Controller and possible "Recipients"?

Special characteristics of the data controller

What is the business object of the Controller? (e.g. medical center)

Ease of identification

Direct or indirect identification?
Pseudonymisation?

Number of individuals (?)

…a breach can have a severe impact on even one individual

ENISA has produced recommendations for a methodology of assessing the severity of a breach

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

Accountability and record keeping

- GDPR ar. 33 para 5 – The principle of accountability in prctice

The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

- Controllers are obliged to keep an **internal register of data breaches**, regardless of whether a breach should be notified to the Authority.
- This register is used, inter alia, **to demonstrate compliance** in case of an audit.
  - Therefore, all evidence proving compliance must be recorded (e.g. any risk assessment that led to a decision not to communicate the incident)
- Controllers should investigate each incident, without burdening SAs with information about low risk incidents.

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

Thank you for your attention!