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

Attacks frequently causing data breaches - Organisational and technical measures for preventing/mitigating the impacts

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

(www.bydesign-project.eu)

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

Attacks frequently causing data breaches

- **Ransomware attacks**
  - with or without proper backup and with of without exfiltration
- **Data exfiltration attacks**
  - malicious code, SQL injection, with encrypted or not data
- **Internal human risk source**
  - Intentional exfiltration, accidental transmission
- **Lost or stolen devices and paper document**
  - stolen material with encrypted or not data, stolen paper files
- **Mispostal**
  - snail mail mistake, data sent by email by mistake
- **Other cases – social engineering**
  - Identity theft, mail exfiltration

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

Ransomware attacks

- Malicious code encrypts the personal data.
- Subsequently the attacker asks the data controller for ransom in exchange for the decryption code.
- This kind of attack can usually be classified as a breach of availability, but often also a breach of confidentiality could occur.

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

Case 1. Ransomware with proper backup and without exfiltration

- **Business:** (computer systems of a) small manufacturing company.

- **Case description:**
  - The company used encryption at rest with *state-of-the-art algorithm.*
  - The decryption key was not compromised.
  - Analyzing available logs and detection systems, ***the attacker only had access to encrypted personal data, without exfiltrating it.***
  - Backup readily available - data restored a few hours after the attack took place.
  - No delay in employee payments or handling client requests or consequences on the day-to-day operation.

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

Case 1. Ransomware with proper backup and without exfiltration

- **Affected data/subjects:**
  - Affected data of employees and clients, a few dozen individuals altogether.
  - No special categories of data were affected.
- **Risk assessment:**
  - Confidentiality risks reduced to a minimum - cryptanalytic progress can render the encrypted data intelligible in the future.
  - The breach was unlikely to result in a risk since:
    - the affected data was effectively restored in a few hours from the backup,
    - the breach did not result in any consequences on the day-to-day operation and
    - had no significant effect on the data subjects (e.g. employee payments or handling client requests).

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

Case 1. Ransomware with proper backup and without exfiltration

- **Mitigation and obligations:**
  - Resetting all compromised systems to a clean state known to be free of malicious code.
  - Fixing the vulnerabilities and restoring the affected data soon after the attack.

Actions necessary based on the identified risks		
No risk (internal register)	Risk (notify SA)	High Risk (communicate to data subjects)
✓	X	X

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

Case 2. Ransomware without proper backup

- **Business**: (one of the computers of an) agricultural company.
- **Case description:**
  - Analyzing available logs and other detection systems, ***the attacker only encrypted the data, without exfiltrating it.***
  - No backup was available in an electronic form.
  - Most data were restored from paper backups within 5 working days.
  - Minor delays in the delivery of orders to customers.
- **Affected data/subjects:**
  - Affected data of employees and clients, a few dozen individuals altogether.

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

Case 2. Ransomware without proper backup

Risk assessment:

- Risks from lack of availability as confidentiality is not compromised.
- The likelihood of a confidentiality breach cannot be entirely dismissed
  - sophisticated malware has the functionality to edit log files and remove traces
  - logs are not forwarded or replicated to a central log server,
  - data controller cannot state that the absence of a log entry proves the absence of exfiltration.
- No special categories of personal data affected.
- Low quantity of breached data and number of affected data subjects.
- Absence of a backup database - data still available on paper.

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

Case 2. Ransomware without proper backup

Obligations:

- Notification to SA necessary:
  - data restoration took some time,
  - could cause some delays in the orders' delivery to customers and
  - a considerable amount of meta-data (e.g. logs, time stamps) might not be retrievable.
- Informing the data subjects may depend on:
  - the length of time the personal data is unavailable,
  - the difficulties it might cause in the operation of the data controller as a result (e.g. delays in transferring employee's payments),
  - financial loss for individuals with compromised data (delays in payments and deliveries),
  - their contribution needed for restoring the encrypted data.

Actions necessary based on the identified risks		
No risk (internal register)	Risk (notify SA)	High Risk (communicate to data subjects)
✓	✓	✗

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

Case 3. Ransomware with backup and without exfiltration in a hospital

- **Business:** (information system of) hospital / healthcare center

- **Case description:**
  - The logs show no outward data flow in the timeframe of the attack.
  - After analyzing logs and detection systems, ***the attacker encrypted significant proportion of the data without exfiltration.***
  - Backups were available in an electronic form.
  - Most of the data were restored but this operation lasted 2 working days.
  - Major delays in treating the patients with surgery cancelled / postponed.
  - Lower level of service due to the unavailability of the systems.

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

Case 3. Ransomware with backup and without exfiltration in a hospital

- **Affected data/subjects:**
  - thousand employee and patient records.

- **Risk assessment:**
  - high impact of the data unavailability on a substantial part of data subjects,
  - although backup existed and data could be restored in a few days,
  - a high risk still exists due to the consequences from the data unavailability at the moment of the attack and the following days,
  - residual risk of high severity to the confidentiality of the patient data,
  - high quantity of breached data and number of affected data subjects.

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

Case 3. Ransomware with backup and without exfiltration in a hospital

- **Obligations:**
  - Necessary to notify: special data categories, restoration could take a long time, resulting in major delays in patient care.
  - Necessary to inform data subjects: due to the impact for the patients, even after restoring the encrypted data.
  - Direct communication of the data breach: to the impacted patients i.e. those scheduled to be treated during when the system was unavailable.
  - Public communication or similar equally effective measure: to the other patients (exception of article 34 (3) c).

Actions necessary based on the identified risks		
No risk (internal register)	Risk (notify SA)	High Risk (communicate to data subjects)
✓	✓	✓

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

Case 4. Ransomware without backup and with exfiltration

- **Business:** public transportation company
- **Case description:**
  - The server was exposed to a ransomware attack and data were encrypted.
  - The attacker not only encrypted, but also exfiltrated the data.
  - A backup database existed, but it was also encrypted by the attacker.
- **Affected data/subjects:**
  - Clients, employees and several thousand people using the services of the company (e.g. buying tickets online).
  - Breached data involved basic identity data, identity card numbers and financial data such as credit card details.

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

4. Ransomware without backup and with exfiltration

- **Risk assessment:**
  - Data availability and confidentiality breach.
  - High number of individuals affected and the overall quantity of affected data.
  - High risk from identity documents and financial data.
  - The backup files were affected by the ransomware.
  - The breach presents high risk because it could likely lead to both:
    - material (e.g. financial loss since credit card details were affected) and
    - non-material damage (e.g. identity theft or fraud since identity card details were affected).

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

4. Ransomware without backup and with exfiltration

- **Obligations:**
  - Communication to data subjects essential: they can make the necessary steps to avoid material damage (e.g. block their credit cards).
  - Communication on a person-by-person basis.
  - For individuals where contact data is not available, the controller should do so publicly, e.g. by way of a notification on its website.
  - Precise and clear communication is required, in plain sight on the homepage of the data controller, with exact references of the relevant GDPR provisions.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	✓	✓

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

Ransomware attacks

	Internal documentation	Notification to SA (risk)	Communication to data subjects (high risk)
CASE No. 01: Ransomware with proper backup and without exfiltration	YES	X	X
CASE No. 02: Ransomware without proper backup	YES	YES	X
CASE No. 03: Ransomware with backup and without exfiltration in a hospital	YES	YES	YES
CASE No. 04: Ransomware without backup and with exfiltration	YES	YES	YES

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

Organizational and technical measures for preventing / mitigating the impacts of ransomware attacks

- keeping firmware, operating system and application software on the servers, client machines, active network components, and any other machines on the same LAN (including Wi-Fi devices) **up to date**,
- existence of an up-to-date, secure and tested **backup** procedure,
- appropriate, up-to-date, effective and integrated **anti-malware** software,
- appropriate, up-to-date, effective and integrated **firewall and intrusion detection and prevention system**,
- **training** employees on the methods of recognizing and preventing IT attacks
- forwarding or replication all logs to a **central log server**,
- strong **encryption** and **authentication**,
- **vulnerability** and **penetration testing** on a regular basis,
- establish a Computer Security Incident Response Team (**CSIRT**) or Computer Emergency Response Team (**CERT**) within the organization,
- when assessing countermeasures – **risk analysis** should be **reviewed**

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

Data exfiltration attacks

- Attacks that exploit vulnerabilities in services offered by the controller to third parties over the internet, e.g. committed by way of injection attacks (e.g. SQL injection, path traversal),
- the risk emanates from the action of an unauthorized third party,
- typically aim at copying, exfiltrating and abusing data for a malicious end,
- they are mainly breaches of confidentiality and, possibly, also data integrity

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

Case 5. Exfiltration of job application data from a website

- **Business**: employment agency

- **Case description:**
  - a cyber-attack placed malicious code on the website,
  - the malicious code made the data submitted through online job application forms and stored on the webserver accessible to unauthorized person(s),
  - The malware toolkit was discovered only a month after its installation.
  - The toolkit allowed
    - the attacker to remove any history of exfiltration and
    - processing on the server to be monitored and to have personal data captured.

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

Case 5. Exfiltration of job application data from a website

- **Affected data/subjects:**
  - 213 job application forms were possibly affected,
  - no special categories of data were affected in the breach.

- **Risk assessment:**
  - confidentiality breach with data integrity becoming questionable,
  - the accessed data contains considerable information about the individuals from the online forms,
  - such data could be misused in a number of ways (targeting with unsolicited marketing, identity theft, etc.).

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

Case 5. Exfiltration of job application data from a website

- **Mitigation and obligations:**
  - compare the database with the one stored in a secure backup,
  - return all affected IT systems to a known clean state,
  - remedy the vulnerability,
  - implement new security measures to avoid similar data breaches in the future e.g. file integrity checks and security audits,
  - If personal data were deleted, recover the data in the state they were before the breach,
  - apply full backups, incremental changes and then possibly rerun the processing since the last incremental backup.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	✓	✓

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

Case 6. Exfiltration of hashed password from a website

- **Business**: cooking website

- **Case description**:
  - an SQL Injection vulnerability was exploited to gain access to a server database,
  - users were only allowed to choose arbitrary pseudonyms as usernames,
  - the use of email addresses for this purpose was discouraged
  - passwords stored in the database were hashed with a strong algorithm and the salt was not compromised
  - the controller informed the data subjects about the breach via e-mail and
  - asked them to change their passwords, especially if used for other services.

- **Affected data/subjects:** hashed passwords of 1.200 users

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

Case 6. Exfiltration of hashed password from a website

- **Risk assessment**:
  - data confidentiality is compromised, but passwords were hashed,
  - no contact data (e.g. e-mail addresses or phone numbers) were compromised,
  - no significant risk for the data subjects of being targeted by fraud attempts (e.g. receiving phishing e-mails or fraudulent text messages and phone calls),
  - no special categories of personal data were involved,
  - user names can be regarded as personal data, but the website's subject does not reveal special categories of data (e.g. as political party website).

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

Case 6. Exfiltration of hashed password from a website

- **Mitigation and obligations:**
  - state of the art encryption could mitigate the adverse effects of the breach,
  - limited number of attempts to login will prevent brute force login attacks,
  - use of authentication methods obviating the need to process passwords on the server side is preferable,
  - correct the vulnerability,
  - implement new security measures to avoid similar future data breaches (systematic security audits to the website),
  - strongly advisable to communicate a breach involving passwords to data subjects in any case.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	X	X

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

Case 7. Credential stuffing attack on a banking website

- **Business**: online-banking website
- **Case description**
  - cyber-attack aimed to enumerate all possible login user IDs using a fixed trivial (8-digit) password
  - due to a website vulnerability, in some cases data were leaked to the attacker, even if password was incorrect or bank account inactive,
  - all illegitimate log-on attempts were identified,
  - no transactions were performed by these accounts during the attack,
  - the security operations center detected a high number of login requests,
  - the bank switched off the log in and forced password resets of the compromised accounts,
  - the breach was communicated only to the users with the compromised accounts, i.e. to users whose passwords were compromised or whose data was disclosed.

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

Case 7. Credential stuffing attack on a banking website

- **Affected data/subjects:**
  - affected around 100.000 data subjects,
  - out of these, the attacker successfully logged into around 2.000 accounts which were using the trivial password tried by the attacker,
  - in some cases data were leaked to the attacker: name, surname, gender, date and place of birth, fiscal code, user identification codes.

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

Case 7. Credential stuffing attack on a banking website

- **Risk assessment:**
  - financial data and identity and user ID information,
  - high number of individuals affected,
  - the breached data permits the unique identification of data subjects,
  - contains other information about them (i.e. gender, date and place of birth),
  - can be used to guess the passwords or run a spear phishing campaign,
  - the occurrence of material (e.g. financial loss) and non- material damage (e.g. identity theft or fraud) is a conceivable outcome.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	✓	✓

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

Organizational and technical measures for preventing / mitigating the impacts of hacker attacks

- State-of-the-art **encryption** and **key management**
- **Cryptographic hashing and salting** for secret information (passwords) is always preferred over encryption of passwords
- Keeping the system **up to date** (software and firmware)
- Use of **strong authentication methods** like two-factor authentication and authentication servers
- Up-to-date **password policy**
- Strong **user privileges and access control management** policy
- **Secure development standards**: filtering of user input, brute force prevention measures, WAF
- **Firewall**, **intrusion detection** and other **perimeter defense** systems
- Systematic **IT security audits** and **vulnerability assessments** (penetration testing)
- Regular **reviews** and **testing** to ensure that **backups** can be used to restore any data whose integrity or availability was affected.
- **No session ID in URL** in plain text

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

Internal human risk source

- Common appearance of human error in personal data breaches
- Can be both intentional and unintentional types of breaches
- Difficult for the data controllers to identify the vulnerabilities and adopt measures to avoid them

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

Case 8. Accidental transmission of data to a trusted third party

- **Business**: insurance company and insurance agent
- **Case description**:
  - insurance agent accessed data not belonging to his scope - faulty settings of an excel file received by email,
  - he was the sole recipient of the e-mail,
  - he is bound by professional secrecy and an arrangement with the controller,
  - the agent instantly signalled the mistake to the controller,
  - the controller corrected the file and sent it out again, asking the agent to delete the former message
  - the agent confirmed the deletion in a written statement

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

Case 8. Accidental transmission of data to a trusted third party

- **Affected data/subjects:**
  - two dozen customers,
  - no special categories of personal data,
  - only contact data and data about the insurance itself (insurance type, amount)

- **Risk assessment:**
  - confidentiality breach,
  - low quantity of data affected – no “sensitive” data,
  - immediate detection of the breach and measures taken, deletion of the file

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

Case 8. Accidental transmission of data to a trusted third party

- **Mitigation and obligations:**
  - reducing file exchange through e-mail,
  - double checking files before sending,
  - separating the creation and sending of files,
  - additional steps in checking documents involving personal data

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	X	X

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

Organizational and technical measures for preventing / mitigating the impacts of internal human risk sources

- Periodic **training**, **education** and **awareness** programs for employees
- Effective data protection and privacy **practices and procedures**
- Making proper **access control policies** and forcing users to follow the rules
- **User authentication** when accessing “sensitive” personal data
- **Disabling** user account as soon as the person leaves the company
- **Checking unusual dataflow** between the file server and employee workstations
- Setting up **I/O interface security** in the BIOS or through the use of software controlling the use of computer interfaces (lock or unlock e. g. USB/CD/DVD etc.)
- **Reviewing** employees’ access policy
- **Disabling** open **cloud** services
- **Forbidding** and preventing **access** to known **open mail services**
- **Disabling print screen** function in OS
- Enforcing a **clean desk policy**
- Automated **locking all computers** after a certain amount of inactivity

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

Lost or stolen devices and paper documents

- A frequent case is the loss or theft of portable devices
- measures prior to the breach to ensure an appropriate level of security
- always breach of confidentiality
- If there is no backup, can also be breach of availability and integrity
- the risk assessment might be difficult, as the device is no longer available

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

Case 9. Stolen material storing encrypted personal data

- **Business**: children's day-care center
- **Case description**:
  - two tablets were stolen during a break-in,
  - the tablets contained an app which held personal data about the children attending the day-care center,
  - both the encrypted tablets which were turned off at the time of the break-in, and the app was protected by a strong password.
- **Affected data/subjects**:
  - name, date of birth, personal data about the education of the children attending the day-care center

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

Case 9. Stolen material storing encrypted personal data

- **Risk assessment**
  - Data confidentiality on the devices was not compromised due to the strong password protection on tablets and apps.
  - Due to the measures taken, data confidentiality was kept intact.
  - The backup ensured continuous data availability.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	X	X

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

Case 10. Stolen material storing non-encrypted personal data

- **Business:** service provider company

- **Case description:**
  - The electronic notebook device of an employee was stolen.
  - Access to the notebook's hard drive was not protected by any password.
  - Personal data could be restored from daily backups available.

- **Affected data/subjects:**
  - The stolen notebook contained names, surnames, sex, addresses and date of births of more than 100000 customers.

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

Case 10. Stolen material storing non-encrypted personal data

- **Risk assessment:**
  - Confidentiality breach of the data stored on the stolen device.
  - No password protection or encryption.
  - Lack of prior basic security measures enhances the risk level.
  - High risk of identity fraud.
  - No special categories of personal data.
  - Not possible to identify if other data categories were also affected due to the stolen device unavailability.

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

Case 10. Stolen material storing non-encrypted personal data

- **Mitigation and obligation:**
  - Turning on device encryption.
  - Use of strong password protection of the stored database.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	✓	✓

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

Organizational and technical measures for preventing / mitigating the impacts of loss or theft of devices

- Turn on **device's encryption** (such as Bitlocker, Veracrypt or DM-Crypt).
- Use **passcode/password** on all devices. Encrypt all mobile electronic devices requiring complex password for decryption.
- Use **multi-factor authentication**.
- Turn on **location functionalities** of mobile devices to located them in case of loss or misplacement.
- Use **MDM** (Mobile Devices Management) software/app and localization. Use anti-glare filters. Close down any unattended devices. Enable the remote wipe function.
- Save personal data on a **central back-end server** and not on a mobile device.
- Use a **secure VPN** to connect mobile devices to back-end servers.
- Proper **regulation of device usage** inside and outside the company.
- Use **centralized device management** with minimum rights for the end users to install software.
- Install **physical access controls**.
- **Avoid storing sensitive information** in mobile devices or hard drives

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

Mispostal

- The risk source is an internal human error.
- It is the result of inattentiveness.
- Little can be undertaken by the controller after it happened, so prevention is even more important.

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

CASE 11. Snail mail mistake

- **Business:** retail company

- **Case description:**
  - Two orders for shoes were packed by the retail company.
  - Due to human error two customers got each other's orders, including the packing bills containing the personal data.
  - After becoming aware of the breach the data controller recalled the orders and sent them to the right recipients.

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

CASE 11. Snail mail mistake

- **Affected data/subjects:**
  - The bills contained the personal data required for a successful delivery (name, address, plus the item purchased and its price).

- **Risk assessment:**
  - no special categories of personal data or other data whose abuse might lead to substantial negative effects were involved,
  - the breach is not a result of a systemic error,
  - only two individuals are concerned,
  - no negative effect on the individuals could be identified.

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

CASE 11. Snail mail mistake

- **Mitigation and obligations:**
  - The controller should provide for a free return of the items and the accompanying bills,
  - should request the wrong recipients to destroy / delete all eventual copies of the bills containing the other person's data

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	X	X

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

Case 12. Sensitive personal data sent by mail by mistake

- **Business:** employment department of a public administration office
- **Case description:**
  - An email message – about upcoming trainings - was sent to the individuals registered in the system as jobseekers.
  - By mistake, a document was attached containing all jobseekers' data.
  - The office contacted all recipients and asked them to delete the previous message and not to use the information contained in it.
- **Affected data/subjects**:
  - Name, e-mail address, postal address, social security number of more than 60000 individuals.

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

Case 12. Sensitive personal data sent by mail by mistake

- **Risk assessment:**
  - considerable number of affected individuals,
  - the social security number, along with basic data, increases the high risk,
  - the eventual distribution of the data by any of the recipients cannot be contained by the controller
- **Mitigation and obligations:**
  - the means to effectively mitigate the risks are limited,
  - the controller asked for the deletion of the message but cannot force the recipients to do so,
  - as a consequence, cannot be certain that they comply with the request

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	✓	✓

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

Organizational and technical measures for preventing / mitigating the impacts of mispostal

- **Setting exact standards** for sending letters / e-mails.
- Adequate **training** for personnel on how to send letters / e-mails.
- When sending e-mails to multiple recipients, they are listed in the **'bcc'** field by default.
- **Extra confirmation** is required when sending e-mails to multiple recipients, and they are not listed in the 'bcc' field.
- **Automatic addressing** instead of manual.
- **Disabling autocomplete** when typing in e-mail addresses.
- **Awareness** sessions on **most common mistakes** leading to a personal data breach.
- **Training sessions** and **manuals** on **how to handle incidents** leading to a personal data breach and who to inform (involve DPO).

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

Other cases – social engineering
Case 13. Identity theft

- **Business**: telecommunication company
- **Case description:**
  - the contact center receives a telephone call from someone that poses as a client
  - the supposed client asks to change the email address of the billing info
  - the client's identity is validated and the operator makes the requested change
  - the procedure does not foresee any notification to the former email contact
  - the legitimate client asks why he is not receiving billing to his email address,
  - and denies any call asking the change,
  - later, the company realizes that the information has been sent to an illegitimate user and reverts the change

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

Case 13. Identity theft

- **Risk assessment:**
  - billing data can give information about the data subject's private life (e.g. habits, contacts) and could lead to material damage (e.g. stalking, risk to physical integrity),
  - the data obtained can be used to facilitate account takeover in this organization or exploit further authentication measures in other organizations
  - the "appropriate" authentication measure should meet a high bar, depending on what personal data can be processed as a result of authentication

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

Case 13. Identity theft

- **Mitigation and obligations:**
  - the methods used for authentication were not sufficient,
  - use of static knowledge-based authentication is not recommended,
  - verify the change demand, by sending a confirmation request to the former contact
  - adding extra questions and requiring information only visible on previous bills

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	✓	✓

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

Thank you for your attention!