SECURITY BREACHES

A security breach is any incident that causes the destruction, loss or accidental or unlawful modification of personal data transmitted, stored or otherwise processed, or the unauthorised communication of or access to the data.

Inform the Spanish SA of the breach.

Notification deadline.

- With no undue delay.
- A maximum of 72 hours from becoming aware of it.
- After 72 hours have elapsed, a reasonable explanation must be provided.

Obligation to report the breach.

It is obligatory for any CP, whenever the security breach may cause damages or losses to DATA SUBJECTS or third parties during the data processing, such as:

- Loss of control over personal data.
- Restriction of rights.
- Discrimination.
- Identity theft.
- Financial losses.
- Unauthorised reversal of pseudonymisation.
- Damage to the reputation.
- Loss of confidentiality of the data subject to professional secrecy.
- Any other significant economic or social loss pertaining to a natural person.

Reasons for not reporting breaches.

- When it is improbable that the personal data infringements constitute a risk to the rights and freedoms of DATA SUBJECTS.
- This improbability must be based on the principle of proactive responsibility: being able to demonstrate compliance with all principles of the processing: Lawfulness, Purpose limitation, Data minimisation, Accuracy, Storage limitation, Integrity and Confidentiality.

Contents of the notification

- Nature and context of the breach.
- Possible effects and consequences of the breach.
- Corrective measures implemented or proposed by the CP to remedy and/or mitigate the impact.
- Whenever possible:
    - Categories and numbers of affected DATA SUBJECTS.
    - The categories and number of registers affected.
    - If necessary, the identity and contact information of the DPO or other contacts to obtain more information.
    - If it is not possible to provide all of the information in one communication, it shall be reported in stages without undue delay.

Inform the DATA SUBJECT of the breach.

Notification deadline.

- With no undue delay.

Obligation to report the breach.

- It is obligatory for any CP, when it is probable that it present a HIGH RISK to the rights and freedoms of the DATA SUBJECT.
- Whenever the CP is requested to do so by the SA.

Reasons for not reporting breaches.

- When appropriate technical and organisational protection measures have been adopted applied to make the affected data unintelligible to unauthorised personnel.
- When subsequent measures that guarantee that a HIGH RISK to the rights and freedoms of the DATA SUBJECT is no longer probable.
- When it would suppose a disproportionate effort. In this case, a public communication is possible, which is equally effective for informing the DATA SUBJECT.

Contents of the notification

- A description of the nature of the breach.
- Possible consequences of the breach.
- Corrective measures implemented or proposed by the CP to remedy and/or mitigate the impact.
- If necessary, the identity and contact information of the DPO or other contacts to obtain more information.

Cases of security breaches

A security breach may occur when, for whatever reason, whether intentional or not, the security of the data is violated or it is anticipated that it entails a HIGH RISK to the rights and freedoms of the natural persons.

Access to unauthorised data

- A processing assignment without the corresponding contract.
- Indiscriminate access to printers, photocopiers, etc.
- Unauthorised access to confidential information. For example, payroll data, curriculums, embargoes, video surveillance images, etc.
- Unauthorised access to IT systems.

Communication of unauthorised data

- Unlawful data transmission to a RECIPIENT.
- Breach of professional secrecy.
- Publication of images without the DATA SUBJECT's permission.
- Sending of massive quantities of emails without concealing recipients (blind copies).
- International data TRANSFER without being subject to an EU Sufficiency Decision or suitable data protection

guarantees.

Data alteration

- Malicious modification of data.
- Data falsification.
- Ineffective retrieval of back-up copies.

Loss of information.

- Misplacement or forgetting support mediums.
- Theft or removal of information.
- Removal of IT applications.
- For transport reasons.
- Reorganisation of the company.
- Destruction of data
- Not using paper shredders or digital erasure.
- Fire, flood or other causes alien to the business.

Absence of security measures.

- Antivirus, anti-spam, anti-malware, anti-ransomware, fireware, encryption, pseudonymisation, etc.
- Identification and authentication to access IT systems.
- Security mechanisms to access furniture or departments with personal data.
- Data displayed to unauthorised persons (reception, monitors, tables, etc.).