Key initiatives in 2023

Code of conduct training

In 2023, 90% of the bpostgroup employees received training (created by the HR and Compliance departments) on the Code of Conduct through in-class sessions for staff without a business email address or through a dedicated e-learning channel for staff with one. Made up of different sections, this training underlined the importance of responsible behavior towards clients and colleagues.

Speak up program

A Speak Up program was launched in 2023 featuring a secure 24/7 reporting channel (confidential or anonymous). All bpostgroup employees were informed by letter and email of the program's launch and how to report incidents. This same information was also communicated via videowalls and posters at all company premises.

4.5 Ensuring the data privacy and security of our clients and workforce

We aim to ensure the security of our employee and stakeholder data by fully applying and in some cases even exceeding international data privacy standards across all global operations.

bpostgroup recognizes that information, whether belonging to bpost or held in trust on behalf of its customers and business partners, as well as the ICT facilities on which it is stored, are critical business assets. It is therefore committed to preserving the confidentiality, integrity and availability of all forms of information used and maintained on behalf of its employees, business partners and customers.

As a consequence, specific policies, standards, guidelines and procedures are developed to help administer and manage the storage and processing of information related to the proper and lawful conduct of business. Addressing all information management activities constituting a threat or risk to ongoing bpost activities, their aim is to ensure that any risk is minimized or otherwise accepted by the appropriate management level.

Moreover, an Information Security Roadmap has been developed, outlining the steps and milestones required to achieve the desired level of information security. As a framework for continuous improvement, this Roadmap is reviewed at least once a year in order to stay ahead of emerging threats and ensure that bpostgroup's security framework remains robust, with the risk of security breaches minimized.

As part of the Information Security Roadmap, a Data Security Governance Program has been set up, covering several topics, such as data discovery & prioritization, governance & policies, techniques & protection measures, or information rights management. Alongside this Program, other initiatives aimed at protecting data and sensitive information are either up and running or planned.

From a privacy perspective, the focus has been put on reorganizing governance, improving incident management and further automating data subject access requests.

Key initiatives in 2023

Data classification policy

As part of the Data Security Governance Program, the Data Classification Policy has been fundamentally reviewed. The aim of this policy is to provide guidance to all stakeholders and help them understand data classification at bpost. Moreover, it helps data owners, business owners, ICT data custodians, contractors and vendors to determine what level of security is required to protect data on the bpost systems for which they are responsible. The classification scheme is based on the internationally recognized CIA triad – Confidentiality – Integrity – Availability.

Data leakage detection program

With the support of an external provider, a data leakage detection program is being deployed, searching for possible leaks of bpostgroup-related data and information. The program consists of:

- Domain Protection via monitoring and detecting malicious domains resembling genuine bpost domains and possibly used for launching phishing campaigns and cyberattacks;
- Dark Web Monitoring: detect and mitigate targeted attacks planned on Dark Web forums, messaging apps, etc.;
- Account Takeover Prevention by monitoring and detecting critical credentials leaks before they are compromised;
- Data Breach Prevention via monitoring, detecting and securing publicly accessible sensitive data before any breach occurs.

Information Security Questionnaire

To comply with the EU NIS-2 Directive (the EU-wide legislation on cybersecurity) and more specifically with the requirements regarding Supply Chain Risk, an Information Security Questionnaire has been developed. Our providers are asked to complete it and, where appropriate, implement extra security measures. As the Questionnaire is based on the ISO27001 Information Security Standard, data security is an integral part.

ICT incident management

bpostgroup has made considerable progress in ICT incident management, including improving the handling of data breaches. As an example, bpostgroup employees' attention is being specifically drawn to data breach incidents in the Code of Conduct.