# Cybersecurity and Privacy

The **protection** and **confidentiality** of our customer and stakeholder data, together with the **security** of our operations, are among our top priorities. This is why they are an integral part of our sustainability strategy.

We're aware we operate in an essential industry for businesses, families, and the whole country. This encourages us to innovate and update the ways we work, to ensure the utmost service and security levels.

We've launched an **ESG (Environmental, Social & Governance) Action Plan** where **cybersecurity** plays a pivotal role. In particular, we have laid out specific **business continuity** and **security** plans, as well as constantly updated procedures. Our management is based on the **ISO 27014 standard**, and we implement ongoing training activities with the support of qualified independent partners.

## Our digital transformation strategy

Our digital transformation strategy has been running for several years now and has been taking up pace to respond to the needs arisen with the pandemic emergency: we have improved interactions, autonomy, and flexibility. At the same time, we're paying increased attention to managing risks associated to online banking services, such as digital crime and fraud.

We manage business continuity, cybersecurity, and privacy building on two pillars: the Data Governance and IT Security area provides data and information management and security while ensuring business continuity, whereas the Privacy area protects the Group's information assets.

Both in everyday business and in defining service innovation strategies, we pay attention to strictly complying with national and international regulations and policies.

## A more secure digital environment

Our main goal is to ensure data and operations security. In order to build a more secure digital environment, we're working on three synergic aspects that complement each other: innovation, new technologies, and continuous improvement.

First of all, we're implementing new working modes, including Open Banking extensions, Advanced Analytics or Blockchain, and we've rolled out a next generation SIEM (Security Information and Event Management) system.

Moreover, we constantly introduce new protections, such as double authentication for our apps or Strong Customer Authentication for online payments with cards. We also raise awareness among our customers by providing information through multiple communication channels, and especially the digital ones (apps, web and e-mail, messaging and ATMs).

Finally, we're members of a number of initiatives focused on preventing cybercrime, including: CERTFin (Italian Financial CERT), a public-private initiative aimed at enhancing management capabilities and resilience in the financial system, and the OF2CEN (Online Fraud Cyber Centre Expert Network) project, within whose framework we partner with Italy's National Police to exchange information in real time.

## Our Security Operation Center

In order to take action timely on data security incidents, a Security Operation Center is operative all around the clock, that takes over and assesses cybersecurity reports. Once the type of incident has been identified, the Center adopts containment and resolution measures and engages the appropriate corporate structures. Wherever necessary, the top management is engaged too, based on the level of seriousness.

Our IT system is subject to controls in compliance with the Bank of Italy regulations, with a frequency relative to the types of issues and needs. The Group follows the ISO 27001 security management system standard.

Incident management is part of the wider crisis management process, which defines the strategies and parties to engage. The most relevant cases require an incident report to be filed with control authorities, including the Bank of Italy.

As an additional guarantee, we have taken out two insurance policies offering full coverage on information security incidents.

Approfondimenti

Protecting data and ensuring information security and business continuity are values we uphold every day, through a structured approach and focused initiatives.

Our information system complies with the European and Italian standards and is subject to regular assessment. We also partner with qualified independent third parties.

With corporate responsibility in mind, information security and privacy are overseen by three functions that report directly to the co-general manager and the CEO: Data Governance and IT Security, Information Technology, and Compliance (Data Protection Officer).

In order to identify potential business risks and develop appropriate strategies to minimize them, we conduct a business impact analysis. The impact analysis results help us devise a Business Continuity Plan that ensures the Group's business continuity and defines its principles, procedures, and resources.

To deal with the different scenarios outlined in laws and regulations, the Plan is divided into specific plans, such as the disaster recovery plan, that identifies backup sites and allows relevant procedures to keep working. The Business Continuity Plan is tested at least once a year and its results are presented to the Boards of Directors of the mother company and its subsidiaries.

With respect to the Security Plan, we carry out regular assessments in line with the NIST Cybersecurity Framework standard and in partnership with qualified third parties. Our corporate information system complies with external accreditations (PCI-DSS, SWIFT CSP, etc.) and with Italian and European standards.

We define principles, procedures and resources that ensure business continuity, and we have laid out specific plans to protect operations also in case of adverse events.

## Focus on training

With the aim of raising awareness about security and privacy topics, we implement training initiatives in virtual classrooms, remote or in-person courses, tips and recommendations conveyed to customers and colleagues through our websites, our social media channels and our corporate intranet.

These initiatives touch upon all the most relevant cybersecurity and privacy aspects, starting with general themes and insights into regulations, such as the GDPR. Specific training initiatives on these topics are rolled out to newly hired staff to help raise their awareness.

We also raise their attention toward these types of risks by carrying out simulations of a phishing plan and a mailing that recreates the features of this type of fraud, enabling employees to check them out more easily.

## Data protection framework

Our data protection framework ensures the protection of rights and freedoms of data subjects striking a balance between them and business needs.

The Data Protection Officer (also Data Protection Officer/DPO) is the Head of Compliance Department and reports directly to the CEO and has direct access to corporate bodies.

To support the work of the DPO, Banco BPM created an office specifically dedicated to the world of privacy, to ensure the compliance with data protection regulations in all fields of the business, with an approach that guarantees the treatment of data in respect of the rights and freedoms of data subjects.

Our data protection policy defines: (i) principles and rules to be followed in the day-to-day business, and (ii) roles and responsibilities in the control of the data lifecycle.

All our employees receive guidelines and training on how to process and store data as well as instructions on actions to be taken or avoided to ensure the confidentiality of information.

The organization, acquisition, design and development of an IT component, product or service must also be evaluated for the impact it has on privacy and on the processing and protection of personal data.

Technical and organizational measures, by default, must ensure that only personal data necessary for each specific processing purpose are treated, considering the amount of data collected, the type of processing and their availability.

Our policy on the management of the rights of data subjects provides: i) the constant updating of the Privacy Policy and the identification of the competent business functions responsible for the correct identification of the legal bases for processing such data; ii) the definition of the process for receiving, evaluating and processing requests from data subjects; iii) the synergy with the competent business and technical functions to ensure that the process is properly handled.

Our suppliers guarantee their compliance with data protection regulations and any failure to provide adequate guarantees will result in their exclusion from cooperation.

We promote employee knowledge and awareness through training initiatives consisting of both distance courses and virtual classroom training sessions: solutions that, combined, allow us to involve the largest number of 'Stakeholders' (employees).

Our data breach policy requires the immediate cooperation of all relevant functions in the analysis and classification of incidents and defines the requirements for eventual notifications both to the competent authority and to data subjects.

Our customers can easily manage their privacy preferences, thanks to an *ad hoc* section in the private area of their home banking (App and Web). Here, they can autonomously modify their privacy consents and select their preferred contact channels. For clients without home banking access, however, the management of their privacy preferences and contact channel is handled by the branch with the support of the DPO's dedicated office.

For further information, please consult our privacy section:

https://gruppo.bancobpm.it/privacy