

## NEXI DATA PROTECTION NOTICE

**CONTENTS**

1 USER PRIVACY IS FUNDAMENTAL FOR THE NEXI GROUP..... 3

2 PERSONAL DATA COLLECTED BY NEXI..... 3

3 USE OF PERSONAL DATA ..... 4

4 DATA SUBJECT’S RIGHT TO ACCESS AND CHECK THE PERSONAL DATA..... 5

5 DATA DELETION ..... 5

6 SECURITY MEASURES..... 6

## 1 USER PRIVACY IS FUNDAMENTAL FOR THE NEXI GROUP.

Nexi prioritises relationships with its clients, taking, from the initial stages of service design and development, all the organisational, technical and security measures needed to safeguard the personal data of subjects involved in managing its services (clients, employees and suppliers) in complete compliance with EU Regulation 2016/679 (the “GDPR”) and in line with the most recent best practices for the use of the information systems that make it possible for such services to function properly

Indeed, our mission is to earn and increase our clients’ trust every day, in accordance with the following fundamental principles of data protection:

- Transparency: we provide transparent information on the collection and use of data;
- Security: we protect the data entrusted to us with sophisticated security solutions;
- Control: clients have control over their privacy with easy-to-use instruments and clear options.
- Reporting: we provide periodic disclosures of any reports of data breaches in the consolidated non-financial statement pursuant to Legislative decree no. 254/2016.

Nexi operates in the field of payment services and electronic money management. Therefore, it offers its clients and the clients of its partner banks and companies Issuing and Acquiring services for payment cards (e.g., transaction management), in addition to banking-related services (e.g., wire transfers).

References to Nexi services contained in this notice include the use of websites, apps, servers and various devices made available to clients for the provision of such services.

With this notice, Nexi intends to explain why and how the Group Companies process personal data.

## 2 PERSONAL DATA COLLECTED BY NEXI

Nexi collects a client’s data directly from the client (i.e., data collection from the data subject) and from third-party sources (e.g., its partner banks in order to sell services to end clients, national and international payment circuits, etc.).

In the case of the former, Nexi collects the client’s data when the contracts are signed (e.g., general personal information like the client’s name and contact information and financial information like their IBAN and payment card number, etc.) and subsequently, based on and following the client’s use of the services provided (e.g., data regarding transactions, authentication on Nexi apps, etc.) or when the client requests assistance with any questions or to report issues that arise in the use of the services.

Nexi collects a client’s data from third parties as well, both to meet legal obligations, such as from public databases or authorised parties (e.g., the Company Register, Cerved) when clients are surveyed in accordance with anti-money laundering regulations, and in the course of ordinary operations, such as from national and international payment circuits

(PagoBancomat in Italy and Visa, MasterCard, etc.) for transaction authorisation and accounting.

Moreover, Nexi also collects information on users' visits to its institutional website, portals and apps using technical, analytical and statistical cookies, which by their nature do not require the user's consent, and profiling cookies for marketing purposes, which, unlike the aforementioned cookies, require the user's explicit consent before they may be installed.

### **3 USE OF PERSONAL DATA**

Nexi collects and processes the data and information necessary to provide its services and comply with the related legal requirements, for which it does not need to obtain the data subject's consent.

Nexi obtains explicit consent from the data subjects for certain types of activities like marketing.

In some cases, the data may be used without the data subject's consent in order to conduct statistical, quantitative and qualitative analyses and to meet Nexi's specific needs (legitimate interest) including, but not limited to, analysing its clients' transactions to update its offer to the market, analysing the performance of its applications, searching for new technological solutions to improve the client experience, etc. The outputs of these analyses are aggregate and Nexi uses them to examine and identify trends in its products and/or services, study and develop new products and/or solutions and improve promotions in line with clients' needs and expectations.

Nexi could use the data and information collected for purposes other than those for which they were collected, such as marketing, in compliance with the principles of data protection regulations currently in force, specifically the obligation to inform the data subject of these other purposes and the data subject's rights, including the right to object.

Given the nature of the services provided, the processing of personal data for the purposes indicated above is mainly automated but may include manual processing by the appropriately authorised personnel. These two methods complete one another for the provision of the services.

Automated processing entails using the best technologies available on the market and implementing multiple security systems (e.g., firewalls, credentials, tokens, etc.) to prevent the unintentional and/or temporary loss or unavailability of the personal data processed. To ensure this is accomplished, Nexi has set up specific internal procedures for the initial development and implementation of the applications based on several levels of authorisation for their activation in the production environment.

Manual processing is carried out based on the procedures that Nexi has established for its personnel and the personnel of third parties that the Group Companies may use, with the

support of ongoing general and specialised training provided remotely and in person, according to the assigned duties.

The data are mainly processed electronically. However, some hard-copy processing remains, such as for the management of complaints and disputes, etc.

Nexi shares the personal data collected with suppliers operating on its behalf, which are appointed as data processors in accordance with article 28 of the GDPR, or with other controllers, to meet either operating needs (e.g., payment circuits) or legal obligations (e.g., tax authorities).

Suppliers must process the data exclusively for the purposes of performing their contract with Nexi and are required to inform Nexi of all the operating methods they apply for compliance with the GDPR, such as keeping a record of the processing, appointing any sub-suppliers as processor, the contractual clauses used for any transfers to third countries, etc. In any case, all suppliers are subject to periodic checks by Nexi in order to assess data protection risk.

#### **4 DATA SUBJECT'S RIGHT TO ACCESS AND CHECK THE PERSONAL DATA**

Data subjects may check the personal data that Nexi has collected and exercise their data protection rights by contacting the Data Protection Officer via the channels made available over time and published in the Privacy section of the [www.nexi.it](http://www.nexi.it) website. Nexi's Compliance & AML Manager is the Data Protection Officer (DPO).

In particular, data subjects may request access to their data and the rectification, integration or erasure of their data and the restriction of processing in any of the circumstances provided for by article 18 of the GDPR. They may also object to processing under article 21 of the GDPR.

Furthermore, data subjects may exercise their right to data portability pursuant to article 20 of the GDPR, i.e., the right to receive the data in a structured, commonly used and machine-readable format and, where technically feasible, the right to transmit those data to another controller without hindrance.

Lastly, data subjects have the right to file a complaint with the Personal Data Protection Authority.

#### **5 DATA DELETION**

Nexi retains the collected data solely for the amount of time necessary to provide the services for which the data are stored and, therefore, the data are deleted when no longer used in accordance with the provisions of the GDPR and other legal obligations (e.g., article

2220 of the Italian Civil Code regarding the management of contractual documentation), normally within 10 years of the end of the continuous relationship or earlier if such data were used for specific activities, such as managing disputes with the payment circuits.

## 6 SECURITY MEASURES

For the adequate and secure management of the personal data that the Company collects, stores or processes in any other way, Nexi has established a data protection governance system that ensures compliance with the regulatory requirements in place over time and the security measures adopted, in accordance with the principle of accountability (article 24 of the GDPR).

This governance system consists of Policies, Rules, Operating Procedures and Manuals that are periodically updated to reflect the most recent applicable regulatory requirements and in line with the Company's organisational structure.

The security measures that the Company has adopted are organisational, procedural and technical. They are mainly prepared by the appointed departments under the DPO's supervision.

With specific regard to the definition and implementation of technical measures, the Compliance Department and the DPO are supported by the CISO Area, which is the company department responsible for overseeing information security, the governance of business continuity and security incident management processes and monitoring the effective application of security standards and processes.

The main security measures cover all aspects of data and information security, as regulated by the main standards for the sector, such as secure software development and maintenance, data backup and disaster recovery, logical and physical access management, protection against cyberattacks (e.g., firewalls, anti-malware, etc.) and so on.

Ad hoc security measures are implemented for the processing of hard-copy data and documents, with specific regard to their secure use and storage (e.g., clean desk policy), to protect against the loss of integrity and ensure they are disposed of in accordance with the law when no longer useful or necessary, etc.

The security measures are defined taking a risk-based approach, in accordance with the principles of accountability and privacy by design and by default, and considering other applicable standards and regulations in the sector, such as the security requirements that the Company must meet to maintain its PCI-DSS certification, which often overlap and complement each other. These measures are reviewed and updated whenever necessary to ensure that the data are processed in compliance with current data protection regulations.

Last update: 31 March 2021