PERSONAL DATA PROTECTION POLICY FOR THE USE OF THE APP

Updated on 04.08.2025

1. YOUR PRIVACY

Intesa Sanpaolo S.p.A. cares about your **privacy.** Through our **App**, you can operate quickly and easily, wherever you are, with high standards of **security** and **confidentiality**.
Here we provide you with detailed information on **how we process and protect your personal data when you download and use the Intesa Sanpaolo Mobile App and the Services that you have subscribed to and that we provide through the App.**
As the data controller**, Intesa Sanpaolo S.p.A.**, with registered office in Piazza San Carlo 156, 10121 Turin, Italy, processes the personal data resulting from the installation and use of the App necessary for its **correct use and safe operation**.

This policy complements the Client policy that has already been provided to you, in accordance with **European Regulation 2016/679 ("GDPR - General Data Protection Regulation")**, available at www.intesasanpaolo.com (Privacy section), where we covered general topics of privacy and confidentiality of personal data.

2. WHAT PERSONAL DATA DO WE PROCESS?

The regulations define "**personal data**" as information that identifies you or makes you identifiable as a natural person.

The personal data we process and protect when you use our App fall into the following categories:

a. **Information about the device you use**, such as the type (e.g. smartphone/tablet), operating system (e.g. iOS/Android), language settings, telephone or internet provider, network connection address (IP address), date, time, other installed applications with their "technical details" and the so-called unique identifiers (i.e. codes and numbers that are used to uniquely distinguish one device from another and are provided by the device manufacturer);

   With regard to the 'technical details' of other applications installed on your device, the only data we process are those strictly necessary for the identification of any 'malicious' Apps, to ensure IT security and prevent fraud. We do not collect statistics or usage data on other Apps you have installed, nor do we carry out profiling activities on such data. All this is done with the aim of protecting you and your data and enabling us to comply with the regulations to which we are subject as a banking institution.

b. **Information on your location (so-called geolocation)** taken directly from your device or entered by you, following your request to use certain services such as searching for the nearest fast cash machines (you can find more details on this in section 6 of this document;

c. **Other information processed by the App:** depending on the services you request from us, we may process certain data obtained through the features of your device that the App may ask access to, such as:

   - Your **contacts** in the address book – to facilitate the execution of operations such as phone top-ups;
   - Data contained in the **memory** - e.g., to allow you to save or open documents;
   - Data on your **call system** - to make calls directly from the App;
   - Data on your **push notification system** - to be able to send you push notifications useful for authorising current account orders and operations such as, for example, credit card payments;
   - Data contained in the **calendar** to save deadlines in your agenda;
   - Data contained in the **photo gallery** - for example, to retrieve images of documents.

   The fingerprint or facial recognition **authentication functionality**, which may be enabled to operate on the App without entering the owner code and PIN, is carried out by

software installed on the device by the manufacturer and therefore does not involve the processing of biometric data in the procedures managed by the Bank.

3. WHY DO WE NEED TO PROCESS YOUR DATA?

We need your data to enable safe and proper functioning of the App and the services you have activated.

If you decide not to provide us with all or part of these data, you might not be able to use the App or some of its features.

This can happen for two main reasons:

1) some permissions are necessary to provide you with the services and features you've activated, which make your operations easier and faster. For example, if you don't allow us to access your camera, you won't be able to make a "cardless" withdrawal (without a physical card) because you need to scan the QR Code that appears on the ATM screen with your camera;
2) as a banking institution, we must comply with regulations concerning fraud prevention and cybersecurity. In these cases, processing certain data related to your device is mandatory for us. The only way to prevent such processing, since these are regulatory obligations we are subject to as a Bank, is not to download and use the App.

We want to assure you that we only process technical data from your device and installed Apps, strictly adhering to best practices (Google and Apple Store Guidelines, where we distribute our Apps), only when you use our App and solely to protect you from malware and fraud.

4. HOW DO WE COLLECT YOUR DATA?

The data we process may be obtained:

Directly: you provide them to us by logging in and using the App.

Indirectly: we have collected them from your device through analysis by the software within the App and also through the **camera** and/or **microphone** functionalities if you have allowed access.

The data we collect are sent to our systems and analysed and archived.

We do not collect information on how you use other apps, and we do not perform profiling activities based on this type of data.

5. WHAT IS THE BASIS FOR OUR PROCESSING? FOR WHAT PURPOSES DO WE PROCESS DATA?

We can only process your data if the purpose of the processing is supported by a legal basis under the GDPR.

We will briefly explain the processing we carry out and the purposes for which we do so.

THE LEGAL BASIS	*OUR PURPOSES*
a) Contract and pre-contractual measures *(Art. 6.1(b) of the GDPR)*	We provide **the services you are entitled to, having signed a contract** with the Bank and other Group Banks and **that you wish to request from us** more easily and quickly via the App. We guarantee **high standards of service** by detecting any anomalies (e.g., abnormal opening of the App, a link or section thereof, or through so-called geolocation, unusual or suspicious access to it from a country other than the one from which you usually access it) and thus avoiding disruptions.
b) Legal obligation *(Art. 6.1(c) of the GDPR)*	We assess the **risks of fraud** and prevent them, as required by EU and national law. We recognise **transactions suspected of being fraudulent and/or attempted fraud** perpetrated against clients, by means of **an automated decision-making process, including profiling.**

6. HOW DO WE COLLECT DATA ON YOUR LOCATION?

We can detect your position (so-called geolocation):

- when you manually enter an address, city or postcode on the App
- via your device's sensors, such as Bluetooth, Wi-Fi, GPS, accelerometer, gyroscope. If present and enabled in the settings, these sensors share the information collected with the device and thus with the App and allow geolocation information to be obtained
- via the Internet connection address (IP address)

This information is **only** detected **when you are using the App**.

You can always disable this information from your device settings or limit it by only activating location tracking while using the App or by only providing us with your address and postcode.

7. PROFILING AND AUTOMATED DECISION-MAKING PROCESSES FOR FRAUD PREVENTION

We take care of your personal data and process them using IT tools with **methods related to the purposes of the processing** described above and we guarantee their **security and confidentiality**.

In order to prevent the risk of fraud, we have developed a **model that processes some data collected by the App through the use of statistical algorithms that allow a predictive assessment of any anomalies** in the operation of the App. Data are analysed and processed by applying a **profiling technique** which allows effective fraud prevention.

This profiling, which is based on the data collected from your device and, only if you have authorized its processing, on information related to your location, is carried out by means of a **fully automated**

decision-making process, i.e., it makes **decisions using technological means, without any human intervention**.

In particular circumstances, for example, when the operating system or the device on which the App is installed are compromised, the fully automated fraud prevention decision making process may go as far as to temporarily inhibit your use of the App.

To ensure the fairness and correctness of this fully automated decision-making process **the method for assessing the reliability and security of the device undergoes regular checks** and we have defined appropriate measures to ensure the proper functioning of the statistical models used and the correctness of their calculation logic over time.

Automatic decisions made by the system to allow you to securely execute banking transactions are made in fulfilment of specific obligations under European Union law and domestic law, aimed at ensuring the prevention, investigation and detection of fraud. The processing of personal data in this case finds its legal basis in article 22, par. 2, letter b) of the Regulation.

8. HOW LONG DO WE KEEP YOUR DATA?

We retain your data for a period of 12 months from when we collected them. The data retention periods stipulated in the Client policy already in your hands do not change.

9. WHO COULD RECEIVE THE DATA YOU PROVIDED?

We may disclose your personal data to the **Intesa Sanpaolo Group Banks** with which you have a current account relationship or another relationship linked to the My Key service, **only for the specific purposes indicated in the policy according to the legal bases provided by the GDPR**.

10. YOUR RIGHTS

As also specified in our general policy, if you wish to obtain **more information on the processing of your personal data** or to **exercise your rights** under the GDPR, you can send a request in writing to the Data Protection Officer at dpo@intesasanpaolo.com or by PEC at: privacy@pec.intesasanpaolo.com attaching the Form for the exercise of rights that you can find in the "Privacy" section of the website www.intesasanpaolo.com.

GLOSSARY

IP Address: is a unique number used by Browser, Device and App to connect to the Internet. This number is generated by the provider of your Internet connection service and allows identification of the provider and/or the approximate geographical area in which you are located as well as your identification. Without such data you cannot connect to the Internet, and we use it to provide you with the Services but also to collect information about your location.

Unique Identifiers: this is information that can uniquely identify you through your Device and/or Application. Advertising identifiers provided by manufacturers such as Apple's IDFA and Android's AAIG are considered as included in this category. On this topic, we would like to point out that, in line with the opinions of the European Supervising Authorities, we do not use other Unique Identifiers such as MAC Address and IMEI as you cannot reset them. To find out how to reset or not share Unique Identifiers with us, go to the section "Set your preferences for Data collected by Device and Application".

Software Development Kit (SDK) and related technologies: this is information that applications record and/or read on your device. Typically, these technologies allow the use of an application to be analysed.

Aggregated information: this is statistical information extracted and filtered (free of your personal data) so that it is no longer traceable to you. We use this information to measure the effectiveness of our services.

Geolocation and Device Sensors: these are sensors such as accelerometer, gyroscope, Bluetooth, Wi-fi and GPS that, if enabled within the device settings, share the information collected with the App and allow us to obtain information on your location.