Updated on 26/01/2026

PERSONAL DATA PROTECTION NOTICE

Summary

1. Your privacy

At **Intesa Sanpaolo S.p.A.** we know the value of your personal data and we constantly strive to process them confidentially and securely so that you, who are interested in our products and services, may entrust them to us with peace of mind.

This privacy notice is provided to you pursuant to Articles 13 and 14 of the GDPR (General Data Protection Regulation - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016) and concerns the personal data you provide to us – including with regard to guarantors, legal representatives, or other individuals possibly connected to your request – to request the initiation of the opening of an account or another contractual relationship, or to request the execution of an occasional transaction. The notice describes the processing carried out during the preliminary stage of your request, necessary to assess the request itself and to manage the related relationships with the people involved.

In this notice we will show you which categories of data we handle and why; which data sources we draw on; how we process your data, with whom we share it and for how long we store it. We will then review each of your rights, set forth in the GDPR (General Data Protection Regulation - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016), providing you with the information you need to exercise them.

If your request is successful and the contractual relationship is established or the occasional transaction is carried out, you will be provided with a new notice that will replace this one and will contain a complete description of the processing related to the management of the contractual relationship and the provision of the requested banking services.

We are at your service to ensure adequate, timely and rigorous protection of your data.

2. To whom is this notice addressed?

To each of our potential clients; and therefore to you who have contacted us to open an account or another contractual relationship, or to request to carry out a one-time

transaction, and are interested in receiving information about our products and services offerings.

The notice is also addressed to all those who, in various capacities and with reference to your request, are connected to you (for example, legal representatives, administrators, partners, beneficial owners, attorneys, delegates, or signatories) or to your guarantors.

Its content may concern you as a natural person, sole proprietor or freelancer.

We may need to amend or supplement it, due to regulatory obligations or as a result of organisational changes. You may consult the latest version at any time in the "Privacy" section of our website www.intesasanpaolo.com.

If you become our customer, you will receive an additional information notice, which will replace this one, regarding the processing we will perform to manage the relationships you have established or wish to establish and to carry out any occasional transactions you may decide to make.

3. What is data processing? who is the data controller?

The GDPR defines "personal data" as "any information relating to an identified or identifiable natural person".

The GDPR also defines precisely what is meant by "processing", namely "any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".

As the "Data Controller", Intesa Sanpaolo, acting in full compliance with the principles of fairness, lawfulness and transparency, determines the means and purposes of each of these "operations" that involve, even only potentially, your personal data; it does all this while ensuring your confidentiality and fully protecting your rights.

4. What personal data do we process?

The personal data we process and protect fall into the following categories:

a. identification and personal data, such as your name and surname, business name, tax code, VAT number, date and place of birth, address of residence/domicile, tax domicile, correspondence address, gender, nationality and data relating to identification documents;

b. image data, such as a photograph on an identification document;

c. contact details, such as landline and mobile phone numbers, ordinary and certified e-mail addresses;

d. other data, provided when requesting a specific product or of the request to carry out an occasional transaction.

5. From whom do we collect your data? how do we process them?

We need your information to start the process of opening your account or contractual relationship, to initiate the execution of the occasional transaction you intend to carry out, to provide you with the requested information about our products and services, and to comply with legal obligations.

If you decide not to provide us with your data, we will be unable to proceed with opening your account and responding to your request for information and/or contact.

6. What is the basis for our processing? for what purposes do we process your data?

The data we process may originate:

Directly: if you provided them;

Indirectly: if we have collected them from third parties or from sources accessible to the public, in compliance with the relevant regulations.

We take care of your data in any case: we process it using manual, computer, and telematic tools – including artificial intelligence systems, as defined by current

regulations – and we ensure its security and confidentiality. In some cases, we may also process your data using profiling techniques, in compliance with the principles of the GDPR. Specifically, if profiling activities are aimed at fulfilling legal obligations, we adhere to the criteria set out by the relevant regulations.

The methodology and logic of the profiling processes carried out for fraud prevention and IT security monitoring are described in the attachment "Profiling for anti-fraud purposes and IT security monitoring."

7. What is the basis for our processing? For what purposes do we process your data?

The processing of personal data is only lawful if its purpose is supported by a valid legal basis, i.e. one of those provided for in the GDPR.

In accordance with the various legal bases provided, we will briefly explain the processing we carry out and the purposes for which we do so for those who, like you, are not yet our clients.

THE LEGAL BASIS	OUR PURPOSES
• Implementation of pre-contractual measures at the request of the data subject (Art. 6.1(b) of the GDPR)	 We carry out activities related to your request to open an account and to obtain information about our products and services and/or to be contacted again.
• Legal obligation (Art. 6.1(c) of the GDPR)	 We comply with regulatory requirements, e.g. anti-money laundering and fraud prevention ones, as well as with provisions of the Authorities.
• Legitimate interest (Art. 6.1(f) of the GDPR)	 We pursue the legitimate interests of ourselves or of third parties, which are shown to be lawful, concrete and specific, after having ascertained that this does not compromise your fundamental rights and freedoms. These include, for example, security of IT systems and networks, prevention of fraud and the production of statistics. The complete list of legitimate interests we pursue is described in the annex "Legitimate interests".

8. Who might receive the data you provided?

We may disclose your data to other parties, both within and outside the European Union, but only for the specific purposes indicated in the notice according to the legal bases provided by the GDPR.

The recipients of your data may be:

a. the Authorities and the parties to whom the communication of the data is due in compliance with regulatory obligations;
b. subjects belonging to the Intesa Sanpaolo Group;
c. parties with whom we have commercial agreements;
d. parties that operate in the following sectors:

- banking, financial and insurance services;
- provision and management of IT and telecommunications procedures and systems;
- computer security;
- freelancing;
- consultancy in general;
- management of customer relations (e.g. in relation to communication and assistance);
- logistics;
- the storage of data and documents (both on paper and electronic media;

A detailed list of the recipients of personal data is available on request.

9. How do we protect your data when we transfer them outside the european union or to international organisations?

We normally process your data within the European Union, but for technical or operational reasons, we may however transfer data to:

- countries outside the European Union or international organisations that have been found by the European Commission to provide an adequate level of protection;
- other countries, in which case we rely on one of the “adequate safeguards” or one of the specific derogations provided for in the GDPR.

10. How long do we keep your data?

The retention period of your data depends on the positive or negative outcome of your request to open an account or another contractual relationship, or to carry out a one-time transaction. In fact, your data is kept for a period of 15 days (after which it is deleted) if the aforementioned request is abandoned or not completed, that is, if within that period the following occurs, depending on the case: the request to open a contractual relationship is unsuccessful and the contract is not concluded; you do not create your personal ACCESS PIN for the APP when the account opening request is made through this channel; the request to carry out a one-time transaction is unsuccessful. We will process your personal data for a longer period only in cases expressly provided for by law or to pursue a legitimate interest, ours or that of third parties.

If, on the other hand, the request concludes successfully – that is, depending on the case, with the opening of the account or another contractual agreement, or with the execution of the occasional transaction – your data is stored in accordance with the Customer Information, which is provided to you at the same time as the account opening or the execution of the occasional transaction.

11. How can you contact us?

These are the details for contacting us:

- Data Controller: Intesa Sanpaolo S.p.A.
- Registered office: piazza San Carlo 156, 10121 Torino
- dpo@intesasanpaolo.com
- privacy@pec.intesasanpaolo.com
- www.intesasanpaolo.com

12. Who is the “data protection officer”? how can you contact him/her?

The “Data Protection Officer" (DPO) is a guarantee figure that we have appointed, as explicitly required by the GDPR. You can contact the DPO for all matters relating to the processing of your personal data and to exercise your rights under the GDPR, by emailing dpo@intesasanpaolo.com

13. What are your rights?

The GDPR grants you the following rights outlined below, which you can exercise in accordance with the specific characteristics of the processing described in this information notice:

Right to object (pursuant to article 21 of the GDPR): if your personal data are processed by us for direct marketing purposes, you have the right to object to the processing and any profiling activities related to them at any time; if you exercise this right, your personal data will no longer be processed for this purpose.

You can also exercise the right to object to the processing we carry out to perform tasks in the public interest, to exercise public powers or to pursue a legitimate interest of ourselves or third parties. In such cases, the processing will no longer be carried out unless there are reasons that oblige us to continue or it is necessary to establish, exercise or defend a right in court.

Automated decision-making including profiling (pursuant to art. 22 GDPR): We do not normally make decisions based solely on automated processing of your personal data except in specific areas and only when the decision relates to the finalisation or performance of a contract, when it is based on your explicit consent or is authorised by law.

In the first two cases (contract and consent) we guarantee your right to obtain human intervention, to express your opinion and to object to the decision.

You always have the right to receive meaningful information on the logic used and the importance and consequences of automated processing.

Right of access (pursuant to article 15 of the GDPR): you have the right to obtain confirmation as to whether or not personal data concerning you is being processed by us, to have information on the processing in progress and to receive a copy of the data.

Right to erasure (pursuant to art. 17 of the GDPR): the GDPR provides for a series of cases in which you have the right to obtain the erasure of personal data concerning you (for example, if you have exercised your right to object to the processing, if the data is no longer necessary for the purposes for which it was processed or if you have withdrawn the consent on which the processing is based and there is no other legal basis for processing it).

Right to restriction (pursuant to art. 18 GDPR): the GDPR provides for a number of cases in which you have the right to request the limitation of the processing of personal data concerning you (e.g. for the period necessary to carry out appropriate checks on personal data whose accuracy you have contested).

Right to data portability (pursuant to art. 20 GDPR): the GDPR provides for a number of cases in which you have the right to receive the personal data you have provided us with and which concern you in a structured, commonly used and machine-readable format. The GDPR also protects your right to transmit those data to another data controller without hindrance on our part.

Right to rectification (pursuant to art.16 GDPR): you have the right to obtain the rectification of inaccurate personal data concerning you, and the integration of incomplete data.

Right to lodge a complaint (pursuant to art. 77 GDPR): if you consider that your data is being processed by us in breach of the law on the processing of personal data, you have the right to lodge a complaint with the competent Data Protection Authority.

Your rights are described in the document "Focus on your rights" available in the "Privacy" section of the website www.intesasanpaolo.com.

14. Contacts and forms for the exercise of your rights

In the "Privacy" section of the website www.intesasanpaolo.com you will find a form that you can use to exercise your rights.

To exercise your rights, you may write to:
dpo@intesasanpaolo.com
privacy@pec.intesasanpaolo.com;
Intesa Sanpaolo S.p.A., Piazza San Carlo, 156 – 10121 Turin, Italy

We will carry out all necessary actions and communications free of charge. Only if your requests prove to be manifestly unfounded or excessive, in particular due to their repetitive nature, may we charge you a fee, taking into account the administrative costs incurred, or refuse to comply with your request.

15. Annex 1 - legitimate interests

Article 6.1(f) of REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 27 APRIL 2016 (GDPR - General Data Protection Regulation) authorises us to process personal data concerning you without the need to ask for your consent, where the processing is necessary for the pursuit of a legitimate interest of ourselves or third parties, provided that the interest does not override your interests or fundamental rights and freedoms.

With this document, we provide you with an up-to-date list of legitimate interests of ourselves or of those of third parties that we pursue in connection with our operations.

We remind you that, pursuant to article 21 of the GDPR, you have the right to object to the processing of personal data concerning you at any time, if the processing is performed for the pursuit of our interests, including profiling.

Should you object, we will refrain from processing your personal data further unless there are legitimate reasons to proceed with the processing (reasons that override your interests, rights and freedoms), or the processing is necessary for the establishment, exercise or defence of legal claims.

For comprehensive information on the rights that the GDPR recognises in relation to the processing of your personal data, please refer to the "Focus on your rights" document in the "Privacy" section of the website www.intesasanpaolo.com.

List of legitimate interests:

- monitoring the security of IT systems and networks to protect the confidentiality, integrity and availability of personal data;
- adoption of the appropriate safeguards to prevent fraud and mitigate other risks (e.g. with regard to anti-money laundering) required to fulfil legal obligations of the Data Controller;
- exercise of a right in any place;
- transmission of personal data within the group of companies for internal administrative purposes;
- processing of personal data belonging to third parties in the context of the performance of agreements and/or contracts with the Bank's counterparties, inclusive of the pre-contractual phase;

- development and updating of predictive and descriptive models through the production of statistics and reports with the following aims:

1. definition of new products and services;
2. verification of the performance of products and services for their improvement;
3. verification of the effectiveness of processes and/or the operation of units;
4. data quality improvement;
5. construction of general models of potential client behaviour based on statistical analysis of quantitative/qualitative information with the aim of maintaining standards of the offer of products and services high enough to meet client demands;
6. improving user experiences on websites and apps.

16. Annex 2 - profiling for anti-fraud purposes and it security monitoring

For the purposes of preventing and combating fraud, identity theft, and for the security of IT systems, the Bank may collect client behavioural data and carry out profiling activities to identify suspicious or anomalous activities. Personal data are collected through various channels and may also concern registration for banking services, their use and transactional activity.

The personal data used for profiling are specifically processed to pursue the following purposes:

- identification of fraudulent activities to the detriment of the Bank and clients;

- development of predictive models to anticipate potential fraud. These models are built using machine learning techniques and advanced data analysis, based on historical data series of fraud and legitimate transaction data;

- identification of new threats and development of effective defence strategies to strengthen security measures.

We pursue these purposes by monitoring and analysing client transactions in order to identify anomalous or particularly inconsistent behaviour with respect to the client's profile and habits (such as, for instance, the repeated use of a credit card in a short period of time in different locations).

The anti-fraud software used is able to create individual risk profiles based on the behavioural and transactional data of individual clients. These profiles are then used to:

- assess the risk of fraud, including potential identity theft, on the basis of the client's profile;

- customise security measures, implementing specific security controls for each client, based on his or her financial habits.

In case of detection of suspicious activity, automated systems may generate alerts, which are sent to the Bank's security teams for further checks to detect any fraudulent transactions. In some cases, immediate security measures may be

activated, such requesting further confirmations from the client (by means of codes, security questions and, where applicable, identification through the use of biometric data) before proceeding with the execution of the transaction. In higher-risk cases, a temporary suspension of the client's transactions may occur.

The Bank's anti-fraud and IT team intervenes in each case to analyse the reports generated by automated systems, carrying out in-depth investigations to understand the causes of the anomalies detected and to verify the legitimacy of the suspicious transactions.

With regard to profiling carried out for anti-fraud and IT security purposes, we make use of automated systems that analyse data in real-time to monitor client transactions and identify anomalies and fraudulent activities. These systems include behavioural analysis software, machine learning algorithms and artificial intelligence systems.

The personal data processed are those strictly necessary to ensure the accuracy of the analyses, the effectiveness of the systems used and their reliability over time.

To ensure the fairness and correctness of the process employed, we also subject the anti-fraud systems we use to regular checks, so that they remain accurate, effective and non-discriminatory over time.

To this end, we have set up appropriate measures to ensure the proper functioning of the software over time, carrying out periodic updates of the historical series used to build the models, regular checks to ensure the correctness of the data processed, and regular checks on the functioning of the systems used and the quality of the results obtained