PERSONAL DATA PROTECTION NOTICE

1. Your Privacy 1
2. To whom is this notice addressed? 1
3. What is data processing? Who is the data controller? 1
4. What personal data do we process? 2
5. Why are we asking you to provide us with your data? 2
6. From whom do we collect your data? How do we process them? 2
7. What is the basis for our processing? For what purposes do we process your data? 3
8. How do we process your data to assess credit risk? 4
9. Who might receive the data you provided? 4
10. How do we protect your data when we transfer them outside the European Union or to international organisations? 5
11. How long do we keep your data? 5
12. How can you contact us? 5
13. Who is the "Data Protection Officer"? How can you contact him/her? 6
14. What are your rights? 7
15. Why are you being asked for "consents"? 8
16. Contacts and forms for the exercise of your rights 8

Annex 1 - Legitimate interests 9
Annex 2 - Profiled credit risk assessment 11
Annex 3 - Profiling for anti-fraud purposes and IT security monitoring 13
Annex 4 - Notice on international payment transaction processing services provided by Intesa Sanpaolo and SWIFT as joint controllers 14

Updated on 31.03.2025

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 may entrust them to us with peace of mind.

In this notice we will show you which categories of data we handle and why; which data sources we draw on; how we process 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.

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 **clients,** therefore to you who already have a contractual relationship with us, who are about to establish one or who ask us to carry out an occasional transaction.

This notice is also addressed to all those who, in various capacities, have connections with our customers or their guarantors (e.g. legal representatives, directors, shareholders, beneficial owners, attorneys, delegates or signatories).

Finally, this notice is addressed to those whose data have been provided to us by other parties at the pre-contractual stages or in the performance of a contract.

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. In this case, we will notify you through our channels (e.g. apps and internet banking). You may consult the latest version at any time in the "Privacy" section of our website www.intesasanpaolo.com and by using our apps.

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 belong to 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. **data on personal and family situation**, such as marital status and household composition;
e. **financial data**: economic, capital and credit data;
f. **data relating to the relationships you have with us**, such as transaction data, your reference branch, your classification according to the European MIFID Directive and your credit rating;
g. **data belonging to "special" categories**, e.g. biometric data and health data. These are data that were previously defined as "sensitive" and require "special" protection and specific consent;
h. **judicial data** relating to criminal convictions and offences or security measures.

5. WHY ARE WE ASKING YOU TO PROVIDE US WITH YOUR DATA?

We need your data to prepare, conclude and properly perform contracts and to fulfil the relevant legal obligations.

If you decide not to provide us with your data, we will be unable to provide you with our services.

6. FROM WHOM DO WE COLLECT YOUR DATA? HOW DO WE PROCESS THEM?

The data we process may originate:

Directly: if you communicated them to us on the occasions when you interacted with us;

Indirectly: if we have collected them from third parties or from sources accessible to the public (e.g. the Chamber of Commerce and Professional Registers), in compliance with the relevant regulations.

We take care of your data in any case: we process them using manual, computerised and telematic tools – including artificial intelligence systems, as defined by current regulations – and we guarantee their security and confidentiality.

In some cases, we may also process your data by means of profiling techniques, in compliance with the principles of the GDPR. In particular, if profiling activities are aimed at fulfilling legal obligations, we adhere to the criteria set forth by the respective regulations.

If profiling takes place as part of a fully automated decision-making process, you will be provided with specific information and, if necessary, we will request your explicit consent in compliance with the provisions of article 22 of the GDPR "Automated individual decision-making, including profiling".

We may also carry out classification or, where necessary, profiling activities based on legitimate interest pursuant to art. 6, paragraph 1, letter f) of the GDPR for purposes preparatory to the execution of corporate or strategic transactions, such as mergers, demergers, transfers of business units, credits or legal relationships, as specified in Annex 1 "*Legitimate interests*".

The methodology and logic of the profiling performed for fraud prevention and IT security monitoring are described in the annex "Profiling for anti-fraud purposes and IT security monitoring", also available in the "Privacy" section of the www.intesasanpaolo.com website.

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 we pursue.

THE LEGAL BASIS	*OUR PURPOSES*
a) Consent *(Art. 6.1(a) of the GDPR and Art. 9.2(a) of the GDPR)* --- **These types of processing are only possible if you have given your consent for the specific purpose.** **You always have the right to withdraw all or part of the consents given.**	We carry out **direct** and **indirect marketing** and **profiling** activities, and in particular: • we perform activities functional to the **promotion and sale of products and services of companies belonging to the Intesa Sanpaolo Group or of third party companies** and conduct **customer satisfaction surveys** both through the use of automated systems for calling or communicating a call without the intervention of an operator and electronic communications (e-mail, SMS, MMS or other), and also through the use of paper mail and telephone calls through an operator; • by processing your information (e.g. current account transactions, changes in your financial situation, location and movements) and the identification of categories (clusters) we **assess and predict aspects concerning**, among other things, **interests, preferences, consumer choices and habits**, in order to offer you more personalised and appropriate products and services. We process data belonging to **"special" categories** only if strictly necessary **for specific purposes**, for example for the provision of services and products in the context of social impact and welfare initiatives.
b) Contract and pre-contractual measures *(Art. 6.1(b) of the GDPR)*	We provide the services requested and **perform the contracts** or deeds relating to the **pre-contractual phases**.
c) Legal obligation *(Art. 6.1(c) of the GDPR)*	We comply with **regulatory requirements**, for example in the field of taxation and anti-money laundering, anti-corruption and fraud prevention in payment services. We comply with **Authority provisions**, for example in relation to monitoring of operational and credit risks at banking group level. In particular, if regulatory requirements involve profiling activities, we adhere to the criteria set forth by the respective law provisions.
d) 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, physical security, security of IT systems and networks, prevention of fraud, the carrying out of corporate or strategic operations and the production of statistics. In some specific cases, the processing may involve profiling activities (see annex "Legitimate interests" and "Profiling for anti-fraud purposes and IT security monitoring"). The complete list of the legitimate interests that we pursue is described in the annex "Legitimate interests".

8. How do we process your data to assess credit risk?

European regulations require us to assess and update credit risk, in order to ensure the Intesa Sanpaolo Group's financial stability and capital adequacy. We therefore process your data using **profiling** techniques that enable us to assess and maintain your "financial" health status up to date by calculating the maximum repayment instalment you can afford (affordability and sensitivity) and a risk score (a rating) based on the information we have as well as on your transactions and on possible overdrafts on current accounts you have opened with our Group and, if you authorise us, also on accounts you hold with other banks. The assessment system also uses data that you already provide us with other documents, such as tax returns or financial statements. The indicators calculated in this way will be taken into account, along with other information and parameters, also to:

- provide you with an informed reply when you ask us for a loan, credit line or a credit card;
- assess your reliability and timeliness in making payments, if you have taken out a loan.

The methodology and logic of these processing activities are described in the annex "Profiled credit risk assessment", which is also available in the "Privacy" section of the website www.intesasanpaolo.com.

9. 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) the **public information systems** of public administrations. These include:

- the Bank of Italy Central Credit Register (Centrale Rischi);
- the Central Means of Payment Antifraud Office (UCAMP);
- Public administrative fraud prevention system for consumer credit with specific reference to identity theft (SCIPAFI);
- the Tax Database - Archive of relations with financial operators;

c) parties **belonging to the Intesa Sanpaolo Group**, with which, inter alia, suspicious transaction reports forwarded to the UIF (Financial Intelligence Unit within Banca d'Italia) are shared;

d) parties with whom we have **commercial agreements**;

e) parties which act as our **intermediaries and agents**;

f) parties that operate **in the following sectors**:

- banking, financial and insurance services;
- payment systems and circuits;
- measurement of financial risks to prevent and monitor insolvency risk;
- management of asset and credit recovery;
- tax collection and treasury management;
- physical security (e.g. guard and video surveillance services);
- provision and management of IT and telecommunications procedures and systems;
- computer security;
- the professions (e.g. appraisers, notaries and lawyers, inclusive of litigation services);
- auditing of accounts and consultancy in general;
- service quality surveys and market analysis and research;
- advertising and commercial promotion of products and/or services;

- 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).

Your personal data may be disclosed to the company **S.W.I.F.T. SC**, Avenue Adèle 1, 1310 La Hulpe, Belgium (**SWIFT**), in relation to **international payment transactions** (or financial transactions), for the services it provides on our behalf in the role of joint data controller. In this respect, see the specific policy provided in the annex.

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

10. 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 which, as determined by the European Commission, ensure an adequate level of protection;
- other countries, based, in this case, on one of the "adequate safeguards" or one of the specific derogations provided for in the GDPR.

Furthermore, your data contained in the messages regarding financial transfers (e.g. foreign credit transfers) may be transmitted, for the exclusive purpose of **preventing and fighting terrorism and its financing**, to the public authorities of the United States of America, with which the European Union has concluded a specific agreement[1].

11. How long do we keep your data?

We are legally obliged to keep your data for a period of 10 years from the termination of the contractual relationship or, when they have been collected by virtue of an occasional transaction, from the date of the transaction itself.

We will process them for a longer period only in the cases expressly provided for by law or to pursue a legitimate interest of ourselves or of third parties.

12. 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 – Turin
- dpo@intesasanpaolo.com
- privacy@pec.intesasanpaolo.com
- www.intesasanpaolo.com

You may in any event contact any of our local branches: a list and contact details are available in the "Search for a branch" section of our website www.intesasanpaolo.com.

[1] *O.J. European Union L 195/5 of 27.7.2010.*

13. 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 or the certified e-mail address privacy@pec.intesasanpaolo.com.

14. WHAT ARE YOUR RIGHTS?

The GDPR grants you the following rights:

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.

15. WHY ARE YOU BEING ASKED FOR "CONSENTS"?

As described in section 7, **direct and indirect marketing and commercial profiling actions** carried out by Intesa Sanpaolo S.p.A. ("the Bank") are subject to the existence of specific consents that, if you wish, you may grant to us, thereby allowing us to make our best commercial offers to you.

16. 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.

You may also visit any of our branches.

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.

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 third parties that we pursue in connection with our operations, including, where applicable, by means of **classification** or **profiling** techniques.

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:

- **safeguarding physical security**, understood as the security of people and company assets, including through the acquisition of images and videos in the context of video surveillance systems;
- **monitoring the security of IT systems** and networks to protect the confidentiality, integrity and availability of personal data;
- adoption of appropriate safeguards to **prevent fraud** and **mitigate other risks** (e.g. with regard to corporate administrative liability, anti-money laundering and anti-corruption) required to fulfil legal obligations;
- **the exercise and defence of a right** (including the right of claim), 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;
- **carrying out activities not attributable to the performance of contracts but relevant to client relationships** (e.g. client care and assistance);
- **management of corporate and strategic operations** such as, for example, mergers, demergers, transfers of business units, credits or legal relationships, where necessary also through the analysis of objective parameters (e.g. age, residence, type of products managed) and/or related to the banking transactions of clients (e.g. frequency of use of physical branches or of the online channel) that allow to define the subjective scope of such operations..
- development, customisation and training of **artificial intelligence models**, useful for improving and optimizing the processes of the Intesa Sanpaolo Group;
- **development and updating of predictive and descriptive models** also 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. analysis of client behaviour based on quantitative/qualitative information with the aim of maintaining standards of the offer of products and services high enough to meet client demands;
6. definition of client classification/segmentation parameters preparatory to corporate and strategic operations;
7. improving user experiences on websites and apps;
8. determination of fees on contractual relationships with third parties (e.g. suppliers, agents, etc.).

ANNEX 2 - PROFILED CREDIT RISK ASSESSMENT

European regulations on prudential supervision require banks to assess credit risk internally and to keep this assessment constantly up-to-date in order to ensure their financial stability and capital adequacy including at Banking Group level.[2]

To measure credit risk internally, we have developed models that are also based on an **analysis of current account movements** over a 12-month period.

In particular, we analyse the data that you have provided us with directly or that can be obtained from tax returns, financial statements and any further documentation that may be asked for.

We also use movements on current accounts on the basis of the data obtainable from accounts, including joint accounts, that you hold with us, with Group Banks and, if you have consented, also with other banks not belonging to the Group.[3]

Analysis of this information allows us a more effective assessment of credit risk which we represent with synthetic indicators (such as, for example, the **so-called rating, affordability, sensitivity**), whose values are divided into classes.

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

- to guide you in the choice of the solution best suited to your needs, in compliance with the EBA Guidelines on the granting and monitoring of credit;
- to assess your creditworthiness should you apply for credit. The processing of your personal data is necessary in order to respond to your request;
- to allow us to periodically update ratings and to constantly monitor credit risks, including at Group level, on customers granted credit and on those holding a current account for more than three months (in the latter case, we monitor the potential credit risk deriving from possible account overdrafts). The processing of your personal data is mandatory as it is required by law and does not require your consent;
- with regard to the processing of data from information systems operated by private entities on consumer credit, reliability and timeliness of payments (so-called CIS – Credit Information System), to pursue our legitimate interest in the proper measurement of credit risk and the correct assessment of reliability and timeliness of payments. The processing of your personal data does not compromise your fundamental rights and freedoms and does not require your consent.

If the data in our possession, including those held at other Group Banks, are not sufficient, you may be asked for additional personal data; it is understood that you will be free to choose whether or not to disclose data relating to accounts held with other banks.

---

[2] *The subject is regulated mainly by Regulation (EU) no. 575/2013 ("Capital Requirements Regulation" - CRR), by Directive 2013/36/EU of 26 June 2013 ("Capital Requirements Directive" - CRD IV), by the guidelines adopted by the European Commission, by the European Banking Authority, and by the related implementing rules also issued by the Bank of Italy.*

[3] *The data taken from the accounts you hold with banks outside the Group are those that you have provided to us by delivering your account statements, or by using our account information service. This service is a function of a remote service (My Key for individuals and My Key Business) that enables customers to use an electronic link to acquire information on balances and movements relating to payment accounts, accessible online, that a customer holds with other banks or payment service providers. "Online accessible payment accounts" are the accounts (e.g. current accounts) that a customer can access using a bank's or the payment service provider' s internet/mobile banking service where the accounts are opened.*

As for the profiling carried out for the aforementioned credit risk assessment, we use a model that processes and supplements information from various sources through the use of statistical techniques and credit technology best practices.

In this process, in observance of the rules for granting and managing credit, we use statistical algorithms that enable credit risk to be assessed and predicted with a high degree of accuracy.

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

To ensure the fairness and proper use of the process employed, we also subject the calculation methods we use to regular checks, both internal and external, so that they remain appropriate, effective and non-discriminatory over time.

To achieve this, we have defined appropriate safeguards to ensure compliance with regulatory requirements over time, as well as the proper functioning of the statistical models and the related calculation logic. We carry out periodic updates of the time series data used for the estimation of the models, regular checks to ensure the accuracy of the data processed and regular checks on the functioning of the algorithms used and the results achieved.

ANNEX 3 - 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.

ANNEX 4 - NOTICE ON INTERNATIONAL PAYMENT TRANSACTION PROCESSING SERVICES PROVIDED BY INTESA SANPAOLO AND SWIFT AS JOINT CONTROLLERS

We provide you with information on the processing of your personal data carried out by Intesa Sanpaolo and SWIFT, in their capacity as joint data controllers[4] for international payment processing services.

Notice purposes

Your personal data may be processed as part of SWIFT's transaction processing services, which enable us to send and receive financial messages or files and to pre-validate, track and manage financial transactions. For such processing, Intesa Sanpaolo and S.W.I.F.T. SC, with registered office at Avenue Adèle 1, 1310 La Hulpe, Belgium (hereinafter SWIFT) are joint data controllers.

Legal basis and purpose of processing

We process your personal data on the basis of our legitimate interest in order to ensure the security, efficiency and transparency of financial transactions in which you may be involved.

Pursuant to article 21 of the GDPR, you may object at any time to the processing of your personal data if it is carried out in pursuit of our interests. Should you object, we will refrain from further processing your personal data 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 a legal claim of ours or of third parties.

Categories of personal data

Intesa Sanpaolo and SWIFT process the data relating to those who carry out transactions (e.g. the names of the ordering party, the beneficiary and the respective banks, the bank details, the amount and, if expressed, the reason for payment) to the extent necessary to execute the transactions.

Data retention by Swift

Your personal data are deleted from SWIFT's systems in accordance with SWIFT's data retention and deletion procedures, and in any case when the information is no longer needed to fulfil the purposes for which it was collected.

Recipients to whom SWIFT may disclose your data

Protecting and maintaining the confidentiality of your personal data is central to SWIFT's business. SWIFT will share your personal data with a few categories of third parties when necessary to provide or use transaction processing services (such as SWIFT's clients involved in the transaction or SWIFT's network partners).

Data transfer and retention by SWIFT

In some circumstances, SWIFT may transfer your personal data outside the European Economic Area (EEA) using transfer agreements appropriate to data protection. For resilience, availability and security reasons, SWIFT stores message data in its own data centres located in the EU, the United States and Switzerland. The EU Commission has recognised that Switzerland ensures adequate protection of personal data. In addition, to enable the transfer of personal data from the EEA to SWIFT's operational centre in the United States, SWIFT has signed EU standard contractual clauses with its local entity in the Unites States and has implemented additional technical and organisational measures to ensure that all transfers of personal data are GDPR compliant.

Data protection rights

You can exercise your data protection rights - described in the section WHAT ARE YOUR RIGHTS? of the Intesa Sanpaolo Privacy Policy - by contacting us at the references indicated in the same document,

[4] *This Annex contains the privacy policy referring to the processing of your data carried out by Intesa Sanpaolo and SWIFT as JOINT DATA CONTROLLERS. For the processing of your data carried out by these entities in their capacity as INDEPENDENT DATA CONTROLLERS, please refer to the notice provided by Intesa Sanpaolo (of which this is an annex) and the notice provided by Swift at https://www.swift.com, respectively.*

in the section CONTACTS AND FORMS FOR THE EXERCISE OF YOUR RIGHTS. In addition, you have the right to lodge a complaint with the Italian Data Protection Authority ("Garante").

Contacts and joint data controller agreement (PDPP)

For more information on SWIFT's policies regarding the protection of your data within the context of international payment transaction processing services, you may refer to SWIFT's Privacy and Data Protection Policy (PDPP) and related F.A.Q. published by SWIFT at https://www.swift.com. In particular, the PDPP represent the joint data controller agreement between Intesa Sanpaolo and SWIFT, whose contents are summarised in the aforementioned F.A.Q.

NOTICE TO LEGAL PERSONS, ENTITIES OR ASSOCIATIONS

If you represent a legal person, entity or association, we inform you that consent is required to authorise us to use automated systems for calling or communicating a call without the intervention of an operator and electronic communications (e-mail, SMS, MMS or other) to carry out promotional activities or market research.

The granting of consent authorises the Bank to carry out the same processing also by means of paper mail or telephone calls through an operator.

Updated on 17.02.2023

INTESA SANPAOLO

CONSENT TO THE PROCESSING OF PERSONAL DATA BY NATURAL PERSONS, SOLE PROPRIETORS AND FREELANCERS

Taking into account the Notice provided to me pursuant to articles 13 and 14 of the GDPR, I acknowledge the processing of my personal data for the purposes described in the Notice, under letters b), c) and d) of Section 7 "What is the basis for our processing? For what purposes do we process your data?".

Furthermore, with reference to the processing for the purpose of direct and indirect marketing and profiling referred to in point a) of Section 7 of the Notice,

C2 □ **I give my consent** □ **I do not give my consent**

to the processing of personal data for the purposes of commercial information, direct offers, market surveys or customer satisfaction surveys related to products and services of the Bank and companies of the Intesa Sanpaolo Group;

C3 □ **I give my consent** □ **I do not give my consent**

to the processing of personal data for the purpose of offering products and services of the Bank and Intesa Sanpaolo Group companies specifically identified on the basis of personal profile;

C4 □ **I give my consent** □ **I do not give my consent**

to the processing of personal data for the purposes of commercial information, direct offers, market surveys or customer satisfaction surveys related to products and services of other companies

Date and signature of the data subject or his/her authorised representative

_____

In relation to the processing of special categories of personal data necessary for the pursuit of the purposes set out in point a) of Section 7 of this notice

C6 □ **I give my consent** □ **I do not give my consent**

Date and signature of the data subject or his/her authorised representative

_____

CONSENT BY LEGAL PERSON, ENTITY OR ASSOCIATION CONCERNING COMMUNICATIONS IN PROMOTIONAL ACTIVITIES

With reference to the "Notice to legal persons, entities or associations" delivered to us,

C5 □ **I give my consent** □ **I do not give my consent**

to the use of automated calling or communication systems with or without an operator and of paper or electronic communications (e-mail, telefax, SMS, MMS or other) for the performance of promotional activities or the conduct of market research as far as we are concerned.

Date and signature of representative _____

CLIENT CODE: _____

FIRST NAME, SURNAME, COMPANY NAME: _____

ADDRESS, *REGISTERED* *OFFICE:*

_____