BANCA SISTEMA
WWW.BANCASISTEMA.IT

Banca Sistema S.p.A.
Largo Augusto 1/A,
corner. Street Verziere 13 - 20122
Milano
Tel. 02 802801
Fax 02 72093979

ABI Code: 03158
Banca Sistema - Registered in the Register of Banks
Tax Code and VAT Number: 12870770158 - Share Capital: €15,680,112.60 fully paid up
Parent Company of the Banca Sistema Banking Group, registered in the Register of Banking Groups.
Subject to supervision by the Bank of Italy
Member of the Interbank Deposit Protection Fund and the National Guarantee Fund

PRIVACY NOTICE TO CUSTOMERS PURSUANT TO ARTICLES 13 AND 14 OF REGULATION (EU) 2016/679

I. Data Controller and Data Protection Officer (DPO) 1
II. Purposes, methods, and legal bases of processing, and nature of data provision 1
III. Special categories of data 1
IV. Categories of recipients to whom the data may be disclosed or who may become aware of it in their capacity as data controllers or processor 2
V. Rights of the data subject pursuant to Articles 15 et seq. of the GDPR 3
VI. Privacy Notice regarding the processing of personal data in connection with the fund transfer activities carried out by S.W.I.F.T.. 4
VII. Data retention periods 4
VIII. Notice on the protection of personal data regarding consumer credit, creditworthiness, and payment punctuality 4
IX. Transfer of personal data to third countries 4

I. Data Controller and Data Protection Officer (DPO)

The "Data Controller" is Banca Sistema S.p.A., with registered office at Largo Augusto 1/A, corner of Via Verziere 13 – 20122 Milan. The Data Protection Officer whom the data subject may contact to exercise the rights referred to in Section V below is:
Banca Sistema S.p.A.
Largo Augusto 1/A, corner of Street Verziere 13 - 20122 Milan
Tel. +39 02 802801
Fax. +39 02 72093979
Email address: compliance&antiriciclaggio@bancasistema.it
The Data Controller has appointed a Data Protection Officer ("DPO"), whom you may contact to exercise your rights, as well as to receive any information regarding those rights and/or this Privacy Policy, by writing to: privacy@bancasistema.it
The Data Controller and the DPO, including through designated departments, will handle your request and provide you, without undue delay and in any case no later than one month from receipt of the request, with information regarding the action taken in response to your request.
Please note that if the Data Controller has doubts regarding the identity of the individual submitting the request, it may request additional information necessary to confirm the identity of the data subject.

II. Purposes, methods, and legal bases of processing, and nature of data provision

Banca Sistema S.p.A. (the "Bank") hereby informs you that the personal data in its possession—collected directly from you or from third parties, such as credit brokers and financial agents—may be processed, including by third-party companies, for the following purposes:

1. Compliance with obligations under laws, regulations, and EU legislation, or with instructions issued by authorities legally empowered to do so and by supervisory and regulatory bodies (e.g., obligations under anti-money laundering regulations). The provision of personal data necessary for these purposes is mandatory, as failure to provide such data will prevent the Bank from performing the activity you have requested; therefore, the related processing does not require the consent of the data subjects. The legal basis for the processing is the fulfillment of a legal obligation to which the data controller is subject (Art. 6(1)(c) GDPR).
2. Purposes strictly related to and necessary for the management of customer relationships within the scope of the activities carried out by this Bank in accordance with its Articles of Association and the law (for example, gathering preliminary information prior to entering into a contract, executing transactions based on obligations arising from the contract entered into with the customer, and conducting reviews and assessments of the results and performance of the relationships, as well as the risks associated with them). The provision of personal data necessary for these purposes is not mandatory, but refusal to provide such data may result—depending on the relationship between the data and the requested service—in the Bank's inability to provide the service in question. The processing of such data does not require the consent of the data subjects. The legal basis for the processing is the performance of a contract or the implementation of pre-contractual measures at the request of the data subject (Art. 6(1)(b) GDPR).
3. Purposes related to the Bank's business activities, such as: a) Carrying out activities related to the presentation and promotion of products and services provided by the Bank and other companies within the Group (direct marketing), including via telephone contact or automated systems (email, SMS, MMS, fax) or other communication tools; b) Measuring customer satisfaction with the quality of services provided and the activities carried out by the Bank and other companies within the Group, through in-person or telephone interviews, questionnaires, etc.; c) Promotional initiatives regarding products and services of our Bank, companies within the Group to which we belong, or third-party companies, including the organization of events, also through automated systems (SMS, MMS, fax, and email); d) Disclosure or transfer of data to third parties for the purposes of commercial information, market research, and direct offers of their products and services through the sending of promotional and commercial communications via traditional contact methods (such as calls with an operator and regular mail) and/or automated methods (such as fax, SMS, MMS, and email). The provision of data necessary for these purposes is optional, and their processing requires the consent of the data subjects. The lack of consent will have no consequences on the relationship between the parties, as it may only result in an improvement of the service. Consent may be withdrawn at any time by notifying the Data Controller. The legal basis for the processing is therefore the data subject's explicit and prior consent (Art. 6(1)(a) of the GDPR).

The data is processed using manual, computerized, and electronic means in accordance with procedures strictly related to the aforementioned purposes and, in any case, in a manner that ensures the security and confidentiality of the data.

To provide customers with a more efficient, timely and personalised service, the Controller may use advanced artificial intelligence (AI) technologies, including tools supporting employees in their daily activities and intelligent document management platforms.
In particular, the Controller may use generative AI systems to assist with the summarisation of communications, work organisation and internal document analysis. These systems act as support tools for our employees, helping them perform their tasks more efficiently. The Controller may also use specialised AI tools for the drafting and automated analysis of contractual documentation, ensuring greater accuracy, regulatory compliance and efficiency in the preparation of documents relating to customers.
In addition, the Controller may use AI-based applications to monitor transactions carried out by customers on their accounts and banking relationships, with the aim of promptly identifying unusual or potentially fraudulent transactions and strengthening fraud prevention and detection measures.

Banca Sistema S.p.A.
Largo Augusto 1/A,
corner. Street Verziere 13 - 20122
Milano
Tel. 02 802801
Fax 02 72093979

ABI Code: 03158
Banca Sistema - Registered in the Register of Banks
Tax Code and VAT Number: 12870770158 - Share Capital: €15,680,112.60 fully paid up
Parent Company of the Banca Sistema Banking Group, registered in the Register of Banking Groups.
Subject to supervision by the Bank of Italy
Member of the Interbank Deposit Protection Fund and the National Guarantee Fund

The use of these technologies does not involve solely automated decision-making producing legal effects concerning data subjects without human involvement. Any action suggested by AI is reviewed and validated by a qualified employee before being implemented, and the algorithms operate on verified datasets to reduce the risk of inaccuracies. Likewise, within the fraud monitoring systems, any alerts generated by the applications are used solely as decision-support tools and are reviewed by competent personnel before any action is taken in relation to the customer.
Any personal data processed through AI tools remain within the Bank's secure environment. The Controller has configured these systems in Enterprise mode to ensure that the information processed is not used by technology providers to train their public AI models. All processing activities are carried out on secure servers and in compliance with applicable legal requirements.
In addition to the rights provided for under Articles 15 et seq. of the GDPR, data subjects have the right to request information about the logic involved in the AI systems used by the Controller and to request that any action taken by the Controller be fully reviewed by a human member of staff.

III. Special categories of data

In the course of its ordinary business activities and when providing specific services, the Bank may process information that Article 9 of the GDPR classifies as "special categories of personal data". These include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, as well as data concerning health or a person's sex life or sexual orientation.
Such processing is carried out solely for the purposes and on the legal bases set out below.
A) Incidental and indirect processing in connection with payment services
The Bank may process special categories of personal data only where this is necessary to execute specific services and transactions requested by its customers. This includes the execution and technical routing of payment orders submitted by customers or third parties (such as bank transfers or SEPA Direct Debit (SDD) instructions). In these cases, the Bank may automatically and incidentally store and process special categories of personal data where such information has been entered by the payer in the payment reference or description field, or where it can reasonably be inferred from the nature of the payee (for example, payments to healthcare providers, political parties, trade unions, religious organisations or other entities from which sensitive information about the customer may be inferred).
In these cases, the legal basis for the processing is Article 9(2)(a) GDPR (the explicit consent of the data subject). However, as the technical infrastructure of payment systems does not allow the automatic filtering of payment references or other text associated with individual transactions, customers who choose not to provide, or who withdraw, their consent are requested not to include information revealing special categories of personal data in payment references or descriptions.
Where such information is nevertheless voluntarily included by the customer, or forms part of incoming transactions initiated by third parties, the Bank, acting solely as the technical provider of the payment service, will process such information only to ensure the proper execution of the requested payment transaction and will protect it through appropriate technical and organisational security measures.
B) Transaction monitoring for anti-money laundering and counter-terrorist financing purposes
The Bank may process special categories of personal data for the purpose of monitoring financial transactions and business relationships in order to carry out customer due diligence, mitigate systemic risk and identify suspicious or unusual transactions. This includes checks relating to Politically Exposed Persons (PEPs) and semantic screening of payment references.
In this case, the legal basis for the processing is Article 9(2)(g) GDPR (processing necessary for reasons of substantial public interest), as provided for under the applicable legislation on the prevention of money laundering and terrorist financing (Italian Legislative Decree No. 231/2007, as amended).
Any special categories of personal data processed for these purposes are handled exclusively by the Bank's control functions (Compliance and Anti-Money Laundering departments) and are subject to strict confidentiality obligations. Such information remains within the supervisory and compliance functions and is never shared with the Bank's commercial or sales departments.
C) Arranging and managing insurance cover related to specific lending products (Salary or Pension Assignment Loans, Personal Loans with Credit Protection Insurance, Mortgages and TFS Advance Loans)
The Bank may also process data concerning the customer's health where this is strictly necessary for assessing applications, arranging and managing insurance policies (whether mandatory or optional) associated with specific lending products.
The Bank collects such data solely for the purpose of transmitting them to the insurance company and, where applicable, for managing insurance claims in its capacity as beneficiary under the policy.
The processing is carried out for the following purposes:

- arranging insurance policies that are mandatory by law for Salary or Pension Assignment Loans;
- arranging credit protection insurance policies connected with mortgage loans or advances against End-of-Service Benefits (TFS).

The legal basis for this processing is Article 9(2)(a) GDPR (the explicit consent of the data subject). Providing these data is not mandatory. However, if the customer chooses not to provide them, the insurance company may be unable to issue the required insurance policy and, where such insurance is mandatory by law, the Bank may be unable to complete and finance the requested lending transaction.
Before submitting income documentation (such as payslips), customers are requested to redact any information that is not relevant for the assessment of their application, particularly information revealing trade union membership, religious beliefs or health information that is not necessary for the purposes described above (for example, details relating to the reason for sick leave).
Under no circumstances will the Bank use special categories of personal data for commercial profiling, marketing purposes or creditworthiness assessments.

IV. Categories of recipients to whom the data may be disclosed or who may become aware of it in their capacity as data controllers or processor

In order to carry out its business activities, the Bank may disclose your data to:

- Financial intermediaries or other categories of entities authorized to distribute the Bank’s products and services;
- Entities designated by law (for example, for purposes related to the exercise of functions concerning the administration, assessment, litigation, and collection of taxes:
  - the Revenue Agency; for purposes related to the administration of justice: the Judicial Authorities; for purposes related to the exercise of supervisory, control, and other functions specifically provided for by law: the Bank of Italy, Consob, and IVASS);
- - Interbank Alarm Center (CAI) – a computerized database established at the Bank of Italy, for purposes related to the proper functioning of payment systems;
- - Credit Bureau – an information system managed by the Bank of Italy, for purposes related to the assessment of customers’ creditworthiness and, in general, for the analysis and management of credit risk;
- entities providing banking, financial, or insurance services, including credit guarantee consortia (confidi); this category also includes so-called “benefondi,” an interbank practice that, in the context of check processing, involves communication between the drawee bank and the drawing bank regarding the existence or absence of sufficient funds to cover checks presented for collection;
- companies belonging to the Banca CF+ Group, of which Banca Sistema S.p.A. is a part, as well as subsidiaries or affiliates, including in relation to the anti-money laundering/counter-terrorism obligations set forth in Articles 35 and 36 of Legislative Decree No. 231 of November 21, 2007, No. 231 and subsequent amendments and/or additions (disclosure to intermediaries belonging to the Banca CF+ Group, even if located in third countries, is permitted provided that they apply equivalent measures);

Banca Sistema S.p.A.
Largo Augusto 1/A,
corner. Street Verziere 13 - 20122
Milano
Tel. 02 802801
Fax 02 72093979

ABI Code: 03158
Banca Sistema - Registered in the Register of Banks
Tax Code and VAT Number: 12870770158 - Share Capital: €15,680,112.60 fully paid up
Parent Company of the Banca Sistema Banking Group, registered in the Register of Banking Groups.
Subject to supervision by the Bank of Italy
Member of the Interbank Deposit Protection Fund and the National Guarantee Fund

- entities to whom the Bank offers products and services;
- entities that provide services for the management of the Bank's information systems and software;
- entities that perform services for the collection and processing of data derived from documents or media (e.g., checks, promissory notes);
- entities that process and transmit communications to and from customers (e.g., mailing, email management);
- entities that archive documentation;
- entities that provide customer support (e.g., by telephone);
- ntities involved in the management of payment services and electronic networks, tax collection agencies, and treasury departments;
- entities that operate national and international systems for the detection and prevention of fraud (e.g., involving debit/credit cards or other payment instruments; in the consumer credit sector and for deferred or delayed payments, etc.);
- entities engaged in investigating and combating international terrorism;
- entities engaged in debt collection activities;
- consultants;
- freelancers, public officials, etc. (such as when, for example, the Customer intends to enter into a mortgage agreement or execute a public deed with the Bank, or any other document requiring notarization by a notary public or other public official);
- entities engaged in marketing or market research, or involved in the promotion of the bank's products or those of third parties;
- parties conducting searches—for example, requests to verify the existence of encumbrances (mortgages, sales, etc.) against the Customer at the Land Registry Offices or at the Court Registries (to ascertain whether insolvency proceedings are pending);
- entities that perform control, audit, and certification activities regarding the bank's operations, including in the interest of customers;
- entities acquiring a business, a business unit, a block of identifiable legal relationships, or individual legal relationships (for example, the assignment of receivables);
- entities resulting from the Bank's transformation, merger, or demerger;
- entities managing activities related to the issuance and use of credit, debit, and prepaid cards (e.g., Nexi S.p.A.).

The Bank uses various third parties as its data processors for certain data processing activities. In addition, the Bank acts as an intermediary in the sale of products and/or services on behalf of third parties to whom the data subjects' information must be transferred. Furthermore, the Bank needs to monitor its own operations and the quality of its services, as well as expand its product offerings. To this end, the Bank discloses data regarding its customers to companies that offer such services, so that they may verify directly with the customers whether the Bank has met their needs and expectations or whether there is potential demand for other products and services. Each customer has the right to withhold consent to the Bank for this type of disclosure and for related processing. A similar right may be exercised regarding the disclosure of data to leading third-party companies, to enable them to offer their products. The entities belonging to the categories to which data may be disclosed will process such information as data processors or independent data controllers, in accordance with the law, within the scope of the existing contractual relationship. In addition, the following categories of individuals may become aware of the data in their capacity as persons authorized to process personal data, with respect to the data necessary for the performance of their assigned duties: employees of the Bank or those seconded to it; temporary workers and interns employed by the Bank.

V. Rights of the data subject pursuant to Articles 15 et seq. of the GDPR

The exercise of the rights set forth in this section is not subject to any formal requirements and is free of charge, except in the case of requests that are manifestly unfounded or excessive pursuant to Article 12(5) of the EU Regulation. The Data Controller and the DPO shall be required to provide information regarding the action taken by the data subject without undue delay, and no later than one month from receipt of the request. Extensions are permitted pursuant to Article 12(3) of the EU Regulation. With regard to the processing described in this notice and pursuant to Articles 13(2)(b), (c), and (d), 15, 16, 17, 18, 19, 20, 21, and 22 of the EU Regulation, as a data subject, you may exercise the following rights:

- **the right of access**, that is, the right to obtain from the data controller confirmation as to whether or not personal data concerning the data subject is being processed and, if so, to obtain access to such data;
- **the right to rectification**, which is the right of the data subject to obtain from the controller the rectification of inaccurate personal data concerning him or her without undue delay. Taking into account the purposes of the processing, the data subject has the right to have incomplete personal data completed, including by means of providing a supplementary statement;
- **the right to erasure ("right to be forgotten")**, which is the right that allows the data subject to obtain from the Data Controller the erasure of personal data concerning him or her without undue delay if one of the grounds provided for by law applies;
- **the right to withdraw** previously given consent at any time, without prejudice to the lawfulness of processing based on consent prior to withdrawal;
- **the right to restrict processing** in cases where: 1) the data subject disputes the accuracy of the personal data, for the period necessary for the controller to verify the accuracy of such data; 2) the processing is unlawful and the data subject opposes the erasure of the personal data and requests instead that its use be restricted; 3) the personal data is necessary for the data subject to establish, exercise, or defend legal claims; 4) the data subject has objected to the processing pursuant to Article 21 of the GDPR, pending verification of whether the legitimate grounds of the data controller override those of the data subject;
- **the right to data portability**, that is, the right to receive personal data concerning the data subject in a structured, commonly used, and machine-readable format, and the right to transmit such data to another data controller without hindrance from the data controller to whom the data subject has provided the data, provided that the processing is based on consent or a contract and is carried out by automated means;
- **Right to object**: The data subject has the right to object, at any time, on grounds relating to his or her particular situation, to the processing of personal data concerning him or her where such processing is carried out for the purposes of the legitimate interests pursued by the Data Controller. The Data Controller shall refrain from further processing personal data unless it demonstrates compelling legitimate grounds for the processing that override the rights of the data subject, or for the establishment, exercise, or defense of legal claims;
- **Right to object to direct marketing**: the data subject has the right, in particular, to object at any time to the processing of personal data concerning him or her for direct marketing purposes, including profiling to the extent that it is related to such direct marketing. The Data Controller shall refrain from further processing the personal data for the related purpose.
- **the right to lodge a complaint with the Data Protection Authority** if the data subject believes that their rights have not been respected. The contact information for the Data Protection Authority is available on the website www.garanteprivacy.it;
- to obtain, in the case of automated decision-making, information regarding the logic of the processing in question, as well as to request human intervention by the Data Controller, and to be able to express their opinion or object to the processing itself.

Any corrections, deletions, or restrictions on processing made at the request of the data subject—unless this proves impossible or involves a disproportionate effort—will be communicated by the Data Controller to each of the recipients to whom the personal data has been disclosed. The Data Controller may disclose such recipients to the data subject if the data subject so requests.

To exercise the aforementioned rights and request such disclosure, please contact: Banca Sistema S.p.A., Largo Augusto 1/A, corner of Via Verziere 13 (Tel. +39 02 802801, Fax: +39 02 72093979, email: compliance&antiriciclaggio@bancasistema.it) and to the DPO (see Section I).

Banca Sistema S.p.A.
Largo Augusto 1/A,
corner. Street Verziere 13 - 20122
Milano
Tel. 02 802801
Fax 02 72093979

ABI Code: 03158
Banca Sistema - Registered in the Register of Banks
Tax Code and VAT Number: 12870770158 - Share Capital: €15,680,112.60 fully paid up
Parent Company of the Banca Sistema Banking Group, registered in the Register of Banking Groups.
Subject to supervision by the Bank of Italy
Member of the Interbank Deposit Protection Fund and the National Guarantee Fund

VI. Privacy Notice regarding the processing of personal data in connection with the fund transfer activities carried out by S.W.I.F.T

To process international financial transactions (such as cross-border wire transfers) and certain specific domestic transactions requested by customers (e.g., wire transfers in foreign currency and/or involving non-resident counterparties), it is necessary to use an international messaging service. The service is managed by the "Society for Worldwide Interbank Financial Telecommunication" (SWIFT), with its registered office in Belgium (see www.swift.com for the privacy policy). The Bank provides SWIFT (the operator of the SWIFT Net FIN system) with data regarding the parties involved in the transactions (such as, for example, the names of the payer, the payee, and their respective banks, bank details, and the amount) that are necessary to execute them. At present, banks would not be able to execute the aforementioned transactions requested by customers without using this interbank network and without providing it with the data indicated above.

With regard to the service managed by SWIFT, two key circumstances have come to light: a) All customer data used to execute (all) of the aforementioned financial transactions is currently—for operational security reasons—duplicated, transmitted, and temporarily stored by SWIFT on a company server located in the United States of America; b) The data stored on that server may be accessed in the U.S. in accordance with local law. Competent U.S. authorities (in particular, the Department of the Treasury) have had access to it—and may continue to access it—based on measures deemed permissible under U.S. counterterrorism legislation. This issue is widely debated in Europe among various institutions in relation to the provisions of European data protection law. We also remind you that you retain the rights set forth in Section V above. To supplement the information provided in this document, for a more detailed overview of the activities carried out by Banca Sistema and SWIFT as joint controllers pursuant to Article 26 of the GDPR, we invite you to review Annex 1 to this notice.

VII. Data retention periods

The data processed will be retained for specific periods, as specified below in accordance with Article 13(2)(a) of the EU Regulation. The data processed by Banca Sistema S.p.A. for purposes strictly related to the management of obligations arising from the contractual relationship will be retained for the time strictly necessary to pursue the purposes associated with it and, in any case, for a maximum period of 10 years from the end of the relationship, after which the data will be deleted or anonymized, provided there is no need for further retention for the purposes of legal defense. Upon termination of the relationship, the data will be retained only if necessary to comply with legal requirements, such as tax or anti-money laundering obligations, in addition to any requests for further retention for judicial purposes.

VIII. Notice on the protection of personal data regarding consumer credit, creditworthiness, and payment punctuality

If you apply for a loan or other credit facility, the Bank will use certain personal data relating to you in order to assess your creditworthiness and payment reliability. These data are either provided directly by you or obtained by consulting credit information databases. The relevant information will be retained by the Bank.

In addition, for the purpose of carrying out a more accurate assessment of credit risk, certain information may be shared with the following Credit Information Systems (Sistemi di Informazioni Creditizie – SIC), which operate in accordance with the applicable Code of Conduct for credit information systems managed by private entities concerning consumer credit, creditworthiness and payment reliability: CRIF S.p.A. and Cerved Group S.p.A.

You have the right to access your personal data at any time.

If you apply for a loan or other credit facility, you will also receive a separate privacy notice entitled "Privacy Notice on Credit Information Systems (SIC)", to which reference is made for further details.

IX. Transfer of personal data to third countries

Personal data is not transferred outside the European Union. However, it is understood that, should it become necessary, we may transfer personal data to non-EEA countries, and we hereby guarantee that such transfers will be carried out in compliance with applicable legal provisions:

- in the case of international transfers of personal data originating from the European Economic Area (EEA) and destined for a non-EEA country, the transfer may take place if the European Commission has recognized that a non-EEA country provides an adequate level of data protection: in this case, your personal data may be transferred on this basis;

- for transfers to non-EEA countries where the level of protection has not been recognized as adequate by the European Commission, we may rely on an exemption applicable to the specific situation and/or, in any case, by adopting the standard contractual clauses provided by the European Commission for the transfer of personal data outside the EU.

BANCA SISTEMA
WWW.BANCASISTEMA.IT

Banca Sistema S.p.A.
Largo Augusto 1/A,
corner. Street Verziere 13 - 20122
Milano
Tel. 02 802801
Fax 02 72093979

ABI Code: 03158
Banca Sistema - Registered in the Register of Banks
Tax Code and VAT Number: 12870770158 - Share Capital: €15,680,112.60 fully paid up
Parent Company of the Banca Sistema Banking Group, registered in the Register of Banking Groups.
Subject to supervision by the Bank of Italy
Member of the Interbank Deposit Protection Fund and the National Guarantee Fund

APPENDIX 1 - PRIVACY NOTICE REGARDING INTERNATIONAL PAYMENT PROCESSING SERVICES PROVIDED BY BANCA SISTEMA IN JOINT CONTROL WITH SWIFT

We are providing you with this notice regarding the processing of your personal data by Banca Sistema and SWIFT, acting as joint controllers for international payment processing services.

I. Purpose of Notice

Our 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 this processing, the joint controllers, pursuant to Article 26 of the GDPR, are Banca Sistema S.p.A., with registered office at Largo Augusto 1/A, corner of Via Verziere 13 - 20122 Milan, and S.W.I.F.T. SC, with registered office at Avenue Adèle 1, 1310 La Hulpe, Belgium (hereinafter "SWIFT").

II. Legal Basis and Purposes of Processing

We process your personal data on the basis of our legitimate interest, pursuant to Article 6(1)(f) of the GDPR, 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 for the pursuit of our interests. If you object, we will refrain from further processing your personal data unless there are legitimate grounds for processing (grounds that override your interests, rights, and freedoms), or the processing is necessary for the establishment, exercise, or defense of our rights or those of a third party.

III. Categories of Personal Data

Banca Sistema and SWIFT process data relating to the parties involved in transactions (such as the names of the payer, the payee, and their respective banks; bank account details; the amount; and, if provided, the payment description) to the extent necessary to execute such transactions.

IV. Data retention by SWIFT

Your personal data is 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 necessary for the purposes for which it was collected.

V. Recipients to whom SWIFT may disclose your data

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

VI. Data transfer and retention by SWIFT

n certain circumstances, SWIFT may transfer your personal data outside the European Economic Area (EEA) using appropriate data protection transfer mechanisms. For reasons of resilience, availability, and security, SWIFT stores message data in its data centers located in the EU, the United States, and Switzerland. The EU Commission has recognized that Switzerland ensures an adequate level of protection for personal data. Furthermore, to enable the transfer of personal data from the EEA to SWIFT's operations center in the United States, SWIFT has entered into the EU Standard Contractual Clauses with its local entity in the United States and has implemented additional technical and organizational safeguards to ensure that all transfers of personal data comply with the GDPR.

VII. Data Subject Rights under Articles 15 et seq. of the GDPR

You may exercise your data protection rights—as described in Section V of the aforementioned Banca Sistema S.p.A. Customer Notice—by contacting us at the contact details provided in Section I of that notice.

VIII. Contacts and Joint Controller Agreement (PDPP)

For further information on SWIFT's data protection policies regarding the processing of international payment transactions, please consult the Personal Data Protection Policy (PDPP) and the related FAQs published by SWIFT at https://www.swift.com, in the Knowledge Centre. In particular, the PDPP constitutes the joint controller agreement between Banca Sistema and SWIFT, the contents of which are summarized in the aforementioned FAQs.