# SCALAPAY IP S.P.A. – PRIVACY NOTICE

Scalapay IP S.p.A., a payment institution incorporated under Italian law, with registered office at Via Nervesa, 21, 20139 Milan (MI), Tax Code and VAT No. 06078740484, carrying out its activities pursuant to Articles 114-sexies et seq. of Legislative Decree No. 385 of 1 September 1993 (il "**Testo Unico Bancario**" or "**TUB**"), registered under No. 36018.0 in the Register of Payment Institutions pursuant to Article 114-septies of the CBA and subject to the supervision of the Bank of Italy (hereinafter also "**Scalapay IP**" or "**Data Controller**" or "**Controller**" or "**Company**"), acting as data controller, respects your privacy and is committed to protecting your personal data. Scalapay IP undertakes to process your data in accordance with the General Data Protection Regulation (EU Regulation 2016/679), commonly known as the "**GDPR**", and any other applicable privacy legislation.

This notice sets out the reasons for, and the methods of, collection, management and protection of personal data relating to **customers of Scalapay IP's services, hereinafter also referred to as "Consumers" (SECTION A)**, as well as **to affiliated sellers of Scalapay IP, hereinafter also referred to as "Merchants" (SECTION B).**

In particular, the processing of personal data carried out by Scalapay IP shall be guided by the principles of lawfulness, fairness, transparency, purpose limitation and storage limitation, data minimisation, accuracy, integrity and confidentiality.

Scalapay IP has appointed a Data Protection Officer ("**Data Protection Officer**" or "**DPO**"), who may be contacted by data subjects for information regarding the processing of personal data carried out by the Controller, both with respect to Consumers and Merchants, at the following address: privacy@ip.scalapay.com.

It is important that you read this notice, together with any other notice we may provide to supplement, update or elaborate on the information regarding the collection and processing of your personal data. We will endeavour to coordinate these notices so as to represent, at all times, the conditions applicable to the processing of your personal data in the most transparent and easily accessible manner. In particular, consultation of the Scalapay website and mobile application before opening a personal Scalapay account (the "Scalapay Account") is governed by the privacy notice of Scalapay S.r.l., while the opening and management of the Scalapay Account are governed by the General Terms and Conditions of the Scalapay Account, both available on the website www.scalapay.com.

Scalapay IP adopts appropriate technical and organisational security measures to protect your Personal Data against unauthorised access, loss, destruction or improper disclosure, in line with the state of the art and with the nature of the processing carried out.

* * *

## SECTION A – CONSUMER PRIVACY NOTICE

### 1. DATA CONTROLLER

This notice is drafted pursuant to Articles 13 and 14 of the GDPR and is intended to provide you with information on the manner in which Scalapay IP processes your personal data as data controller. Your personal data are collected through the use of the website www.scalapay.com and the Scalapay app (hereinafter, the "**Scalapay Platform**") when you decide to use one of the services offered by Scalapay IP, through which you, as a consumer (hereinafter also "**Consumer**" or "**Data Subject**"), may purchase products and services from affiliated sellers (hereinafter, the "**Merchants**") through one of the payment services offered by Scalapay IP (e.g.: Pay in 3; Pay in 4; Pay in 6, 9, 12; Pay Later; One Time Card or Pay Now–Cart Saver via one time card or traditional BNPL; Scalapay Club Card). For the purposes of performing the contract concluded with the Merchant, Scalapay IP also processes personal data collected from Merchants and/or from Scalapay S.r.l. Your Personal Data are also collected upon the opening and management of your Scalapay Account, in accordance with the General Terms and Conditions of the Scalapay Account, irrespective of the activation of a specific Service.

The Services are intended for adult natural persons: opening an Account and using the Services are not permitted to persons under 18 years of age.

If you open your Scalapay Account when making a purchase through the Pay Now service, the Account may be created on the basis of a limited set of Personal Data communicated to us directly by the Merchant from which you make the purchase, rather than provided directly by you. Scalapay IP processes such Data as data controller pursuant to Article 14 of the GDPR, since they are collected from a third party (the Merchant) and not from you, for the purposes and on the legal basis set out in Section 2.

**2. PROCESSING DESCRIPTION**

To facilitate understanding of the processing activities carried out by Scalapay IP, we set out below a table containing: (i) the categories of personal data processed, (ii) the purposes of processing, (iii) the "legal basis" that authorises each processing activity and renders it lawful, and (iv) the period of time for which Scalapay IP will retain your personal data (the "**Personal Data**" or "**Data**").

| Category of Personal Data | Purpose of Processing | Legal Basis | Retention Period |
|---|---|---|---|
| Contact and identification data provided when opening the Scalapay Account (first name, last name, tax identification number, e-mail address, mobile phone number, address of residence or domicile), access credentials and data relating to any basic anti-fraud checks. | Opening and management of the Scalapay Account in accordance with the General Terms and Conditions of the Scalapay Account, including access to the Scalapay Platform, management of credentials and authentication mechanisms (e.g., via OTP codes) and basic anti-fraud checks to verify Account ownership, irrespective of the activation of a specific Service. | Performance of a contract to which the Consumer is party, or execution of pre-contractual measures taken at the Consumer's request (Article 6, paragraph 1, letter b) of GDPR); for basic anti-fraud checks, legitimate interest of the Controller in the security of the Account and of its systems (Article 6, paragraph 1, letter f) of GDPR). | For the duration of the Account and, after its closure, for 10 (ten) years, without prejudice to the specific retention periods indicated elsewhere in this table for individual categories of Data. |
| Data communicated by the Merchant when opening the Scalapay Account through the Pay Now service (first name, last name, telephone number, e-mail address, date of birth, gender, country of birth, nationality, country of residence). | Opening and management of the Scalapay Account on the basis of the data made available by the Merchant in the context of the Pay Now purchase process. | Performance of a contract to which the Consumer is party, or execution of pre-contractual measures taken at the Consumer's request (Article 6, paragraph 1, letter b) of GDPR). | For the duration of the Account and, after its closure, for 10 (ten) years, without prejudice to the specific retention periods indicated elsewhere in this table. |
| Consumer contact and identification data, information on goods/services and payment information. For example, first name, last name, tax identification number, residential address (country, province, city, postcode), delivery address, place of birth, date of birth, gender, | Provision of payment services to Consumers (Pay in 3, Pay in 4, Pay in 6, 9, 12, Pay Later or virtual payment card, Scalapay Club Card) and, in particular, the performance of the following activities:<br>– Sending e-mails relating to the transaction;<br>– Transfer of information to the Merchant for performance of the contract; | Performance of a contract to which the Consumer is party, or execution of pre-contractual measures taken at the Consumer's request (Article 6, paragraph 1, letter b) of GDPR). | 10 (ten) years after termination of the contract. |

| Category of Personal Data | Purpose of Processing | Legal Basis | Retention Period |
|---|---|---|---|
| e-mail address, mobile phone number, nationality, identity document (type, number, date of issue, issuing authority, city).<br>Details relating to goods/services purchased or ordered, such as the type of item and the type of Merchant at which purchases are made. | – Providing support upon Consumer request. | | |
| Consumer contact and identification data, data relating to the Scalapay Club Card (card number, expiry date), data relating to transactions carried out with the Scalapay Club Card (amount, date and time, Merchant, product category, country of the transaction), including transactions carried out at merchants not affiliated with Scalapay IP. | Provision of the Scalapay Club Card service, including the authorisation, processing and reporting of payment transactions, as well as the management of the billing cycle and of the monthly balance. | Performance of a contract to which the Consumer is party, or execution of pre-contractual measures taken at the Consumer's request (Article 6, paragraph 1, letter b) of GDPR). | 10 (ten) years after termination of the contract. |
| Biometric data of the Consumer (in particular, derived from the facial characteristics of the Consumer as captured from the selfie or video-selfie taken by the Consumer). | Performing customer due diligence through biometric facial identification of the Consumer. | Legal obligation to which the Controller is subject and pursuit of a public interest (Article 6, paragraph 1, letter c) and e) of GDPR, and Article 9, paragraph 2, letter g) of GDPR, in conjunction with Article 2-sexies of Legislative Decree No. 196/2003 for the purposes of anti-money laundering legislation and fraud prevention, as expressly provided by sector-specific legislation (Legislative Decree No. 231/2007). | 10 (ten) years from completion of the customer due diligence process. |
| Data contained in the Consumer's identity document and selfie or video-selfie taken by the Consumer in the course of the identity verification procedure. | | Legal obligation to which the Controller is subject and pursuit of a public interest (Article 6, paragraph 1, letter c) and e) of GDPR) for the purposes of anti-money laundering legislation and fraud prevention, as expressly provided by sector-specific legislation (Legislative Decree No. 231/2007). | |

| Category of Personal Data | Purpose of Processing | Legal Basis | Retention Period |
|---|---|---|---|
| Image of the Consumer's face. Data contained in the identity document. | Performing customer due diligence - through Alternative Verification (as defined and described in Section 4) - by comparing the image of the Consumer's face with the facial image depicted in the identity document. | Legal obligation to which the Controller is subject and pursuit of a public interest (Article 6, paragraph 1, letter c) and e) of GDPR) for the purposes of anti-money laundering legislation and fraud prevention, as expressly provided by sector-specific legislation (Legislative Decree No. 231/2007). | 10 (ten) years from completion of the customer due diligence process. |
| Images and videos acquired from the Consumer (selfie or video-selfie) and data contained in identity documents. | Carrying out further identity verification checks based on artificial intelligence technologies ("AI") applied to images and videos provided by the Consumer, in order to verify correspondence with identity documents and prevent fraud or misuse of services. | Legal obligation to which the Controller is subject and pursuit of a public interest (Article 6, paragraph 1, letter c) and e) of GDPR), in conjunction with Legislative Decree No. 196/2003, and for the purposes of anti-money laundering legislation (Legislative Decree No. 231/2007) and fraud prevention. | 10 (ten) years from completion of the customer due diligence process or, in any event, until completion of the verification checks through AI. |
| Identification data contained in identity documents (e.g., first name, last name, date and place of birth, date of issue and expiry date of the document), including data collected through automated tools where customer due diligence via biometric identification cannot be successfully completed. | Where the biometric identification process does not allow certain information contained in the identity document (such as the issue date and expiry date) to be properly captured, such data may be acquired through an automated reading system (OCR – Optical Character Recognition). | Legal obligation to which the Controller is subject and pursuit of a public interest (Article 6, paragraph 1, letter c) and e) of GDPR) for the purposes of anti-money laundering legislation and fraud prevention, as expressly provided by sector-specific legislation (Legislative Decree No. 231/2007). | Data is deleted upon completion of the reading process. |
| Identification data contained in the identity document (e.g., first name, last name, date and place of birth, date of issue and expiry date of the document, facial image). | Document verification carried out during the customer due diligence process through an AI-based system. Automated analysis of the document image (prior to the capture of the selfie) to verify its authenticity, integrity and the presence of any signs of tampering or forgery, following its upload by the Consumer. | Legal obligation to which the Controller is subject and pursuit of a public interest (Article 6, paragraph 1, letter c) and e) of GDPR) for the purposes of anti-money laundering legislation and fraud prevention, as expressly provided by sector-specific legislation (Legislative Decree No. 231/2007). | 10 (ten) years from completion of the customer due diligence process. |
| Consumer identification data (first name, last name, tax identification number, date and place of birth, address of residence, identity | Customer due diligence for the purposes of issuing the Scalapay Club Card, in fulfilment of the obligations laid down by anti-money laundering legislation, including the | Legal obligation to which the Controller is subject (Article 6, paragraph 1, letter c) of GDPR), in conjunction with | 10 (ten) years from completion of the customer due diligence process. |

| Category of Personal Data | Purpose of Processing | Legal Basis | Retention Period |
|---|---|---|---|
| document); data relating to employment (type of occupation, sector, type of contract, probationary period); financial and asset data (net monthly income, rent or mortgage, other outstanding financial commitments, total value of assets); source of the funds used; intended use of the Scalapay Club Card; declaration as to politically exposed person (PEP) status. | assessment of the Consumer's risk profile and the verification of the source of funds. | Legislative Decree No. 231/2007, as amended from time to time. | |
| Financial and payment-related data (e.g., last four digits of the card, expiry date and place of issue, IBAN). | Processing payment for the order and managing collections and payments. | Performance of a contract to which the Consumer is party, or execution of pre-contractual measures taken at the Consumer's request (Article 6, paragraph 1, letter b) of GDPR). | 10 (ten) years after termination of the contract. |
| | Management of the AUI (Single Computerised Archive), including reporting activities carried out in fulfilment of regulatory obligations and reporting requirements to the Bank of Italy. | Legal obligation to which the Controller is subject (Article 6, paragraph 1, letter c) of GDPR). | 10 (ten) years from the entry of the report in the system. |
| Consumer identification data (first name, last name, date and place of birth, nationality). | Verification of the Consumer's presence on lists of politically exposed persons (PEPs) and on international sanctions and embargo lists, in the context of enhanced customer due diligence obligations. | Legal obligation to which the Controller is subject (Article 6, paragraph 1, letter c) of GDPR) for the purposes of anti-money laundering and counter-terrorist financing legislation (Legislative Decree No. 231/2007). | 10 (ten) years from completion of the customer due diligence process. |
| Financial and payment-related data (e.g., last four digits of the card, expiry date and place of issue, IBAN) and data relating to purchases already completed. | Management of chargeback requests and disputes relating to payments made by the Consumer, including the necessary checks with the Merchant and with payment service providers. | Performance of a contract to which the Consumer is party, or execution of pre-contractual measures taken at the Consumer's request (Article 6, paragraph 1, letter b) of GDPR). | 10 (ten) years after termination of the contract. |
| Consumer identification and contact data, data relating to the Contracts, to the exposure and to the payment history, requests for forbearance measures and the channel used, signs of payment difficulties (e.g. failed direct debit attempts, overdue instalments on several orders, | Identification of Consumers experiencing payment difficulties, including on the basis of early warning signs; assessment, granting and monitoring of forbearance measures (e.g. deferral or rescheduling of instalments, repayment plans, waiver of late fees); sending of the related communications, including | Compliance with a legal obligation to which the Controller is subject (Article 6, paragraph 1, letter c) of GDPR) under Directive (EU) 2023/2225 on credit agreements for consumers and the relevant national implementing provisions, | 10 (ten) years from the closure of the measure or the refusal of the request; thereafter the data are deleted or anonymised. |

| Category of Personal Data | Purpose of Processing | Legal Basis | Retention Period |
|---|---|---|---|
| repeated requests to postpone instalments), general category of the event that caused the difficulty, essential information on the Consumer's income and on the amount the Consumer is able to pay (only for higher exposures), vulnerable Consumer indicator (yes/no, without indication of the cause), measure requested, granted or refused and related communications. | automated ones; referral to debt advisory se rvices; keeping of the register of measures and internal reporting in aggregate form. | as amended from time to time, and performance of the contract to which the Consumer is party (Article 6, paragraph 1, letter b) of GDPR). | |
| Data provided spontaneously by the Consumer. | Providing responses to Consumer requests, including requests for assistance relating to the Scalapay Account, to the Services used or to the completion of the due diligence process, with the exception of chargeback requests and payment disputes, governed by the preceding row. | Performance of a contract to which the Consumer is party, or execution of pre-contractual measures taken at the Consumer's request (Article 6, paragraph 1, letter b) of GDPR). | For the time necessary to respond to the Consumer and, in any event, for a period not exceeding 2 (two) years. |
| Consumer identification and contact data, data relating to the Scalapay Account and to the Services subject of the complaint, documentation provided by the Consumer in support of the complaint. | Management of complaints relating to the Account and to the Services, including the fulfilments towards the competent out-of-court dispute resolution bodies and authorities where no amicable settlement is reached. | Legal obligation to which the Controller is subject as a supervised intermediary under the applicable rules on banking transparency and out-of-court dispute resolution, as well as performance of contractual measures (Article 6, paragraph 1, letters b) and c) of GDPR). | 5 (five) years from closure of the complaint. |
| All Personal Data indicated in this table (except for biometric data). | Management of any disputes with Consumers. | Pursuit of the legitimate interest of the Controller for the purpose of establishing, exercising or defending a right in legal proceedings, or whenever judicial authorities exercise their judicial functions (Article 6, paragraph 1, letter f) of GDPR). | Until the conclusion of the dispute. |
| Consumer identification and contact data, data relating to the Account and to the Services used, financial and payment-related data, information on the timeliness and regularity of payments. | Assessment of credit, solvency and fraud risk for the purposes of deciding whether to open, maintain or close the Scalapay Account and to provide the Services. | Execution of pre-contractual measures taken at the Consumer's request (Article 6, paragraph 1, letter b) of GDPR). | For the duration of the Scalapay Account and of the Services. |

| Category of Personal Data | Purpose of Processing | Legal Basis | Retention Period |
|---|---|---|---|
| Identification data (first name, last name, tax identification number, date and place of birth), contact details, transaction data, data relating to the request to use instalment payment services, and data relating to payment performance (including any information on late payments or defaults). | Assessment of the creditworthiness and credit risk of the Consumer requesting the use of one of the payment instruments offered by the Controller, fraud prevention, prevention of over-indebtedness and responsible credit risk management.<br>For these purposes, Scalapay IP may:<br>- consult credit information systems and public credit registers ("CIS"), such as the CIS managed by CRIF S.p.A. (Italy), the Fichier national des incidents de remboursement des crédits aux particuliers – FICP managed by the Banque de France (France) and the Central Individual Credit Register managed by the National Bank of Belgium (Belgium), in the cases and for the services indicated in Section 7;<br>- communicate to such CIS data relating to any defaults and to their subsequent regularisation, in the cases and for the services indicated in Section 7. | Performance of a contract to which the Consumer is party, or execution of pre-contractual measures taken at the Consumer's request (Article 6, paragraph 1, letter b) of GDPR), as well as the pursuit of the Controller's legitimate interest in the proper management of credit risk, fraud prevention and compliance with the principles of sound and prudent management (Article 6, paragraph 1, letter f) of GDPR); for France and Belgium, legal obligation to which the Controller is subject (Article 6, paragraph 1, letter c) of GDPR) under the national legislation governing the FICP and the Central Individual Credit Register.<br><br>The processing has been subject to a balancing test pursuant to the GDPR. | Data communicated to the CIS will be processed and stored by such entities in accordance with applicable legislation (for Italy, also with the Code of Conduct for CIS). |
| Data relating to the Consumer's employment and financial situation, collected in the context of a request to use the Pay in 3, Pay in 4 or Pay in 6, 9, 12 services. In particular: type of occupation, type of employment contract, employment sector (public/private), net monthly income, name of employer, completion of the probationary period, existence and monthly amount of fixed financial obligations (rent or mortgage), existence and amount of other active loans or financing arrangements. | Internal assessment of the Consumer's creditworthiness and credit risk in connection with a request to use the Pay in 3, Pay in 4 or Pay in 6, 9, 12 services, for the purpose of determining whether the transaction may be approved, prior to any consultation of Credit Information Systems (CIS) Any vulnerable Consumer indicator is not used for this assessment. | Performance of a contract to which the Consumer is party, or execution of pre-contractual measures taken at the Consumer's request (Article 6, paragraph 1, letter b) of GDPR), and legal obligation to which the Controller is subject (Article 6, paragraph 1, letter c) of GDPR) to carry out a thorough assessment of the Consumer's creditworthiness before concluding the credit agreement, pursuant to Directive (EU) 2023/2225 on credit agreements for consumers and the | 10 (ten) years after termination of the contract. |

| | | | |
|---|---|---|---|
| | | relevant national implementing provisions, as amended from time to time. | |
| Data relating to the provision to the Consumer of the Standard European Consumer Credit Information (SECCI) and of the contract, and to the Consumer's acceptance thereof (including the specific approval of certain contractual clauses, where required by applicable law, and the date and time of acceptance). | Provision of pre-contractual information, conclusion of the contract and retention of evidence of the Consumer's acceptance, in connection with a request to use the Pay in 3, Pay in 4 or Pay in 6, 9, 12 services. | Performance of a contract to which the Consumer is party, or execution of pre-contractual measures taken at the Consumer's request (Article 6, paragraph 1, letter b) of GDPR), and legal obligation to which the Controller is subject under consumer credit legislation (Article 6, paragraph 1, letter c) of GDPR). | 10 (ten) years after termination of the contract. |

| | | | |
|---|---|---|---|
| Identification data.<br><br>Data relating to transactions already carried out using the Controller's services (transaction amount, transaction dates, instalment due dates, payment status). | Analysis of the integration between Scalapay IP's technology and third-party components to achieve the following objectives:<br>- accurate assessment of the creditworthiness and credit risk of Consumers requesting one of the payment instruments offered by the Controller;<br>- proper evaluation of the reliability and timeliness of Consumers' payments;<br>- prevention of fraud risk, including the prevention of identity theft. | Pursuit of the legitimate interest of the Controller (Article 6, paragraph 1, letter f) of GDPR). This processing is necessary to enable Scalapay IP to ensure responsible risk management, prevent fraud and protect Consumers from excessive indebtedness. The processing has been subject to a balancing test to ensure that it does not prejudice the fundamental rights and freedoms of the Consumer. The Consumer has the right to object to such processing at any time by contacting privacy@ip.scalapay.com. | 60 (sixty) days from the risk analysis. |
| Consumer identification and contact data, data relating to transactions carried out with the Scalapay Club Card (including those not converted into BNPL), history of monthly payments and balances. | Assessment and updating of the Consumer's creditworthiness for the purposes of granting and managing the Scalapay Club Card credit limit, including through the consultation of CIS in the cases indicated in Section 7. | Execution of pre-contractual measures taken at the Consumer's request and/or performance of a contract to which the Consumer is party (Article 6, paragraph 1, letter b) of GDPR). | For the duration of the Scalapay Club Card contract and, after its termination, for 10 (ten) years. |
| Contact data (e-mail address, mobile phone number) and data relating to the Services used. | Sending marketing communications relating to Scalapay IP products and services (e.g., newsletters, offers and promotional initiatives) by e-mail, | Consent of the Data Subject (Article 6, paragraph 1, letter a) of GDPR), which may be | Until consent is withdrawn and, in the absence of withdrawal, no |

| | | | |
|---|---|---|---|
| | SMS, push notifications or other channels indicated by the Consumer. | withdrawn at any time without affecting the lawfulness of processing carried out before withdrawal. | longer than 24 (twenty-four) months from the Consumer's last interaction with marketing communications. |
| Contact data (e-mail address) and data relating to the Services already used by the Consumer. | Sending commercial communications relating to Scalapay IP services and products similar to those already used by the Consumer (so-called "soft spam"), without prejudice to the right to object at any time, free of charge and without formalities, both when the data are collected and on the occasion of each subsequent communication. | Legitimate interest of the Controller in promoting its own services and products similar to those already used by existing Consumers (Article 6, paragraph 1, letter f) of GDPR), in accordance with the applicable legislation on electronic communications. | Until the Consumer exercises the right to object and, in any event, no longer than 24 (twenty-four) months from the last transaction. |

**3. THIRD-PARTY LINKS**

The Scalapay Platform, which you access to make instalment purchases at Merchants, may include links to third-party websites (e.g. the websites of the shops where you purchase products or services). By clicking on or enabling such links, third parties may process your Personal Data; accordingly, we invite you to also consult the privacy notices of those sites, as well as the privacy notice of the Scalapay Platform.

**4. IF YOU DO NOT PROVIDE YOUR PERSONAL DATA**

In certain cases, we need to collect your Personal Data by law or under the terms of a contract we have with you or are seeking to enter into with you (for example, to authorise payment deferral). In these cases, failure to provide Personal Data will prevent Scalapay IP from entering into a contract with you.

In particular, in order to comply with the sector-specific legislation applicable to the Company, the provision of Data for biometric verification purposes is mandatory to enable us to perform identity verification online. In any event, where the Consumer is unable, due to technical limitations of their device, to proceed with online identity verification, or has exhausted the identity verification attempts made available by the Company, the Consumer may send an e-mail to support@scalapay.com attaching (i) a photograph of a valid identity document (or equivalent document) and (ii) a photograph showing the Consumer's face and the identity document held in hand. The Company's staff will perform the identity verification manually ("**Alternative Verification**"). In that case, no biometric data of the Consumer will be processed.

With specific reference to the Pay in 3, Pay in 4 and Pay in 6, 9, 12 services, the provision of data relating to employment and financial situation (such as, by way of example, type of occupation, net monthly income, existence of fixed financial obligations and of other active financing arrangements), where requested by Scalapay IP, is mandatory for the purposes of the creditworthiness assessment required under applicable legislation. Failure to provide such data will prevent Scalapay IP from proceeding with the assessment of the request and, consequently, from providing the requested service.

With specific reference to the Scalapay Club Card, the provision of data relating to employment and income (such as, by way of example, type of occupation, sector, type of contract), to the financial and asset situation (such as net monthly income, rent or mortgage, other outstanding financial commitments, total value of assets), to the source of the funds used and to the intended use of the card is mandatory in order to comply with the customer due diligence obligations laid down by anti-money laundering legislation (Legislative Decree No. 231/2007, as amended from time to time). Failure to provide such data will prevent Scalapay IP from issuing the Scalapay Club Card.

If you experience difficulties in paying your instalments, Scalapay IP processes the data necessary to assess and, where appropriate, grant a forbearance measure. You are not required to state or document the specific cause of the difficulty (e.g. health reasons): a general category is sufficient. For higher exposures you may be asked for essential information on your income and on the amount you are able to pay; if you do not reply within 15 days, the request may be refused. If you inform us of a situation of particular vulnerability, Scalapay IP only records an indicator (yes/no), without noting the cause, for the sole purpose of adapting the way you are contacted and assisted: this indicator is not used for the creditworthiness assessment or for marketing purposes. Scalapay IP may deal with a family member or a person you trust only if you have authorised it and after identification.

**5. INTERNATIONAL TRANSFERS**

Some of our suppliers are located outside the European Union. When we transfer your Data to these suppliers, we ensure that your Data are processed and protected in a manner substantially equivalent to the level of protection applicable within the EU. In this regard, in compliance with the safeguards provided for under the GDPR, your data are transferred on the basis of:

- adequacy decisions: where the transfer of personal data takes place to countries that have been deemed by the European Commission to provide an adequate level of protection for personal data;

- standard contractual clauses: in the absence of adequacy decisions, we will use specific contracts approved by the European Commission, designed to guarantee the same level of personal data protection applicable within the European territory.

The list of countries outside the European Union to which Scalapay IP may transfer your data (including information on the safeguards adopted) is available upon request by contacting us at the details indicated in this notice.

**6. TO WHOM WE MAY DISCLOSE YOUR PERSONAL DATA?**

Within the organisation of Scalapay IP, Data may be processed by the employees of the competent departments responsible for carrying out the individual processing activities.

Furthermore, in order to provide our services, we may disclose your Personal Data to the categories of recipients listed below, for the purposes set out herein, in compliance with the principles of minimisation and purpose limitation, and with the implementation of appropriate security measures. The exact identification of the recipients to whom we will disclose your Personal Data will depend on the services you use. In particular, for the provision of services, the categories of parties to whom we will disclose Data, within the scope and limits of the purposes pursued, are:

- Suppliers: we may disclose Personal Data to suppliers – with whom we enter into contractual agreements – that we use to provide you with services. Examples include software and data storage providers, payment processing services, business consultants, companies providing software for biometric facial scanning of Consumers, and affiliation network companies.

- Augusta SPV S.r.l.: Scalapay IP may disclose your Personal Data to Augusta SPV S.r.l., a securitisation vehicle pursuant to Law No. 130 of 30 April 1999, as it is involved in the securitisation transaction for the provision of payment instruments to Consumers.

- Scalapay S.r.l.: Scalapay IP may disclose your Personal Data to Scalapay S.r.l., which develops and manages the Scalapay Platform and the website through which you access your Scalapay Account, acting as data processor on behalf of Scalapay IP, in accordance with the General Terms and Conditions of the Scalapay Account.

- Online and physical stores: Scalapay IP may disclose Personal Data to the online store at which you make a purchase. This is done to enable the store to administer your purchase and your relationship with the store, deliver goods to you, manage any disputes and prevent fraud. Personal data disclosed to a store will be subject to that store's own privacy notice.

- Payment Service Providers ("**PSPs**"): PSPs enable acceptance of electronic payments through a wide range of payment methods, such as credit cards, bank payments including direct debit, etc.

- Debt collection companies: Scalapay IP may need to share your Data upon the sale or outsourcing of recovery of overdue and unpaid receivables to third parties, such as a debt collection company.
- Family member or trusted person: only if authorised by you, in the context of handling a request for a forbearance measure. Scalapay IP also refers you to the debt advisory services available in your country, to which it does not disclose your Data: it is up to you to decide whether to contact them.

- Credit Information Systems (CIS): Scalapay IP may disclose the Consumer's Personal Data to CIS – such as CRIF S.p.A. (Italy), the Banque de France as manager of the FICP (France) and the National Bank of Belgium as manager of the Central Individual Credit Register (Belgium) – in the cases indicated in Section 7, for the purpose of assessing creditworthiness, preventing over-indebtedness and fraud and managing credit risk. These entities act as independent data controllers. The exchange of data with the FICP and with the Central Individual Credit Register may take place through a technical service provider acting on behalf of Scalapay IP.

- Authorities: Scalapay IP may provide information deemed necessary to police, financial, tax or other authorities and courts, including the Bank of Italy or the Revenue Agency. Personal Data are shared with the authority where required by law, in certain cases at your request, or where necessary for the management of tax deductions, the combating of crime or the protection of our rights in judicial or extra-judicial proceedings. An example of a legal obligation to provide information arises where it is necessary to take measures against money laundering and terrorist financing.

Such entities will have access to the Personal Data necessary to perform the functions governed by an agreement between the companies and will act, depending on the circumstances, as independent data controllers or data processors (in the latter case, pursuant to a data processing agreement under Article 28 GDPR).

**7. USE OF CREDIT INFORMATION SYSTEMS ("CIS")**

Depending on the Consumer's country of residence and on the service requested, Scalapay IP may consult and/or communicate data to credit information systems or public credit registers ("CIS"), as described below:

- **Italy** – CIS managed by CRIF S.p.A.: Scalapay IP consults the CIS only where the Consumer requests a service repayable in more than 4 instalments (Pay in 6, 9, 12) and communicates to the CIS data relating to any defaults only in relation to such services. No consultation or communication takes place for the Pay in 3 and Pay in 4 services. Scalapay IP may also consult the CIS for the purposes of granting the Scalapay Club Card.
- **France** – Fichier national des incidents de remboursement des crédits aux particuliers (FICP), managed by the Banque de France: Scalapay IP declares to the FICP the payment defaults relating to any service, where the amounts due remain unpaid for more than 60 (sixty) days after the due date, together with the Consumer's identification data and the amount due, as well as their subsequent regularisation. Scalapay IP consults the FICP only for the Pay in 12 service and for the purposes of granting the Scalapay Club Card.
- **Belgium** – Central Individual Credit Register (Centrale des Crédits aux Particuliers), managed by the National Bank of Belgium: Scalapay IP registers the payment defaults relating to any service, where the amounts due remain unpaid for more than 60 (sixty) days after the due date, together with the Consumer's identification data and the amount due, as well as their subsequent regularisation. Scalapay IP consults the Register for credit requests exceeding EUR 200 (two hundred) and for the purposes of granting the Scalapay Club Card.

In the context of this activity:

- Scalapay IP may disclose to the CIS the Consumer's identification data. Employment and financial situation data collected in the context of the Pay in 3, Pay in 4 and Pay in 6, 9, 12 services are processed exclusively by Scalapay IP for the purposes of the internal creditworthiness assessment and are not disclosed to CIS or any other third parties;
- the CIS may provide Scalapay IP with information on the Consumer's credit profile.

This exchange of information is intended to:

- assess reliability and payment punctuality;
- prevent over-indebtedness;
- prevent and combat fraud or improper use of services;

- ensure responsible and prudent management of credit risk.

Credit Information Systems operate as independent data controllers and process data in compliance with applicable legislation (for Italy, also with the Code of Conduct for Credit Information Systems).

Where required by applicable legislation, the Consumer will be informed before default data are communicated to a CIS for the first time. Where a credit application is rejected on the basis of the consultation of a CIS, Scalapay IP will inform the Consumer, without undue delay and free of charge, of the result of the consultation, of the CIS consulted and of the categories of data taken into account.

The granting of a forbearance measure does not in itself constitute a negative event to be reported to Credit Information Systems; the status of the position communicated to a CIS, where applicable, is updated consistently with the measure granted.

For further information on the manner in which data are processed by the CIS and the related retention periods, the Consumer may consult the privacy notice made available by those entities (for example, on the institutional websites of CRIF S.p.A., of the Banque de France and of the National Bank of Belgium).

**8. FOR HOW LONG WILL WE USE YOUR DATA?**

Further information on the retention period can be found in the table in Section 2. We retain your Data only for as long as necessary to achieve the purposes for which they were collected, such as the performance of the contract or the fulfilment of legal obligations. When deciding how long to retain your Data, we take into account the quantity and type of Data, their sensitivity and the risk of misuse.

At the end of the retention period, Personal Data will be deleted or anonymised. Consequently, once this period has expired, the data subject may no longer be able to exercise the rights referred to in Section 10 (such as the right of access, erasure, rectification and the right to data portability).

**9. BIOMETRIC VERIFICATION PROCESSING. ABSENCE OF AUTOMATED DECISION-MAKING**

The Company uses biometric technologies to perform identity verification of Consumers who wish to use the payment services offered by Scalapay IP. As indicated in Section 2, this processing is carried out to comply with legal obligations in the area of prevention of money laundering and terrorist financing, as required by anti-money laundering legislation (including Legislative Decree No. 231/2007).

Outside the scope of Alternative Verification (which, as indicated in Section 4, applies exclusively in residual cases), the identity verification process is carried out through facial verification technologies based on a one-to-one comparison (between the image of your face captured by the selfie or video and that present in the identity document you provide). To carry out this verification, we will ask you to:

- upload a photograph of your identity document (or equivalent document) directly to the Scalapay Platform;
- take a selfie or record a short video using your device's camera, following specific instructions that ensure correct image capture (e.g., adequate lighting conditions and the absence of other people in the frame).

We will screen your biometric data (the selfie or video referred to above) to verify the correspondence of your face with the photograph in the relevant identity document, verifying the consistency of the information contained in the identity document with that provided by you, as well as the framing and environmental conditions. You will always be aware of the collection of biometric data. Furthermore, Scalapay IP will never – through the process just described – make decisions based solely on automated processing that produce legal effects or similarly significantly affect you. Indeed, where the verification is unsuccessful, the Company's staff will always be involved to assess the reasons.

For further information on the type of technology used by the Company and, in any event, to exercise such rights, please contact our Data Protection Officer (DPO) at the addresses indicated below.

Where automated tools are used for the extraction of data from identity documents, such systems do not autonomously determine the outcome of the verification process, but exclusively support the identification activity, which is completed by authorised personnel or through further controls.

Identity verification procedures also include a check on the reliability of the image of the document provided, both through a comparison of the video and facial images acquired during the identification process with the images present in the document, and through analysis of the elements that make an identity document reliable. These checks are carried out through an AI system, which does not acquire additional data or store information contained in documents. In addition to complying with regulatory obligations regarding the correct identification of the data subject, the checks are intended to prevent possible fraud, for the better protection of services and customers themselves. The AI technologies employed operate in compliance with the principles of lawfulness, fairness, transparency, proportionality and data minimisation, and do not lead to decisions based solely on automated processing that produce legal effects or significantly affect the data subject.

**9bis. ABSENCE OF AUTOMATED DECISION-MAKING FOR CREDITWORTHINESS ASSESSMENT**

In the context of creditworthiness assessment, and in particular for the Pay in 3, Pay in 4 and Pay in 6, 9, 12 services, Scalapay IP may use automated analysis tools that also take into account information from CIS as well as data relating to the Consumer's employment and financial situation (such as type of occupation, net monthly income, fixed financial obligations and other active financing arrangements) provided by the Consumer. In any event, such tools do not result in the adoption of decisions based solely on automated processing that produce legal effects or similarly significantly affect the Data Subject, since adequate human intervention is always provided in cases where this is necessary.

Where the creditworthiness assessment involves automated processing, you have the right to obtain human intervention on the part of Scalapay IP, to receive a clear and comprehensible explanation of the assessment, of the logic involved and of the main factors taken into account, to express your point of view and to request a review of the assessment and of the decision. In the event of rejection of your application, we will inform you without delay of these rights and of how to exercise them.

If an instalment is not paid when due, your Scalapay Account is automatically suspended for new purchases until the overdue instalments are paid. This is a decision based solely on automated processing which is necessary for the performance of the contract (Article 22, paragraph 2, letter a) of GDPR): you nonetheless have the right to obtain human intervention on the part of Scalapay IP, to express your point of view and to contest the decision by contacting Customer Service. Where there are signs of payment difficulties, Scalapay IP may also send you automated communications informing you of the possibility of requesting a forbearance measure and of the debt advisory services: these communications do not involve any decision concerning you.

**10. YOUR RIGHTS**

Please note that you may exercise your rights relating to personal data in the manner and within the limits provided for by data protection legislation. Below is a brief description of such rights, which you may exercise upon satisfaction of the conditions provided for under the GDPR:

- **Right to be informed**: all natural persons have the right to be informed about the collection and use of their Personal Data. This is a fundamental transparency requirement as established by the GDPR. This Notice and the responses we provide to your requests satisfy this requirement.

- **Right to request access to Personal Data**: known as a “subject access request”, this enables you to obtain confirmation as to whether or not processing of Data is taking place and, where it is, to obtain access to the Data and information referred to in the GDPR, as well as to obtain a copy of your Personal Data.

- **Right to request rectification of personal data**: this enables you to correct and supplement any incomplete or inaccurate Data in our possession; however, we may need to verify the accuracy of the new data provided.

- **Right to request erasure of personal data ("right to be forgotten")**: this enables you to request the removal and erasure of your Personal Data where there are no valid grounds for continuing to process them. Erasure of your Personal Data may be obtained in the cases provided for in Article 17 GDPR. However, please note that in certain cases we may be unable to fulfil your erasure request for specific legal reasons (e.g., where erasure is necessary to enable you to comply with a legal obligation or to establish, exercise or defend a right in legal proceedings), which will be communicated to you at the time of your request.

- **Right to object to the processing of personal data**: as provided for in Article 21 GDPR, you may object to the processing of Data, on grounds relating to your particular situation, in cases where we, or a third party, rely on legitimate interests and you consider that such processing adversely affects in some way your fundamental rights and freedoms. In that case, the Company will cease to process the Personal Data further unless the Company demonstrates the existence of compelling legitimate grounds for the processing that override your interests, rights and freedoms, or for the establishment, exercise or defence of a right in legal proceedings. To exercise this right, you may contact us at privacy@ip.scalapay.com.
- **Right to object to marketing and soft spam**: you may at any time, free of charge and without having to give reasons, object to the processing of your Personal Data for direct marketing and soft spam purposes by contacting us at privacy@ip.scalapay.com or support@scalapay.com or by using the unsubscribe link included in each communication. Following the exercise of this right, we will cease processing your Personal Data for such purposes.

- **Right to request restriction of processing of personal data**: you may request restriction of the processing of your Personal Data in the cases provided for in Article 18 GDPR (e.g., where processing is unlawful and you oppose erasure of the Data, requesting instead that its use be restricted).

- **Right to request transfer of personal data to you or to a third party ("data portability")**: we will deliver to you or to a party designated by you your Personal Data in a structured, commonly used and machine-readable format, under the conditions provided for in Article 20 GDPR. Please note that this right applies only to information processed by automated means and to processing carried out on the basis of consent, or in the context of the performance of a contract concluded with you.

- **Right to withdraw consent at any time**: with regard to any processing based on your consent (as collected from time to time by Scalapay IP following provision of an appropriate notice), you will have the right to withdraw at any time the consent given for the processing of Personal Data based on consent, and we will cease to use your Personal Data, without, however, affecting the lawfulness of processing based on consent before its withdrawal.

- **Right to lodge a complaint with a supervisory authority**: please note that you always have the right to lodge a complaint with the Italian Data Protection Authority (Garante per la Protezione dei Dati Personali), with offices at Piazza Venezia 11, Rome, at the e-mail address: protocollo@gpdp.it.

## 11. COOKIES

Scalapay IP does not use any type of cookie on its institutional website (https://paymentinstitute.scalapay.com/). This means that when you browse our website, we do not collect information about your device, such as browsing data or preferences. We do not use third-party cookies for tracking or personalised advertising, and we do not share your information with third parties through the use of cookies.

## 12. CHANGES TO THIS NOTICE

We reserve the right to amend this notice at any time, including to adapt it to legislative or regulatory changes. In the event of material changes, we will inform you with reasonable notice, through the Scalapay Platform or another appropriate channel, before they take effect. We invite you to consult this page periodically to stay up to date.

## 13. CONTACTS

To exercise your rights or to request information about how we process your Personal Data, you may contact us by e-mail at scalapayip@legalmail.it and we will do our utmost to assist you.

Furthermore, if you have questions relating to the processing of Personal Data, including requests to exercise your rights you may also contact our DPO at the following e-mail address: privacy@ip.scalapay.com.

* * *

**SECTION B – MERCHANT PRIVACY NOTICE**

## 1. DATA CONTROLLER

This notice is drafted pursuant to Articles 13 and 14 of the GDPR and is intended to provide you with information on the manner in which Scalapay IP processes your personal data. Your personal data were collected by Scalapay S.r.l. through the use of the website www.scalapay.com and the business platform (hereinafter, the "**Scalapay Business Platform**") or by Scalapay IP when you enter into a contract with Scalapay IP as an affiliated seller (hereinafter also "**Merchant**") in order to offer your customers one of the payment services offered by Scalapay IP (e.g.: Pay in 3; Pay in 4; Pay in 6, 9, 12; Pay Later; One Time Card or Pay Now–Cart Saver via one time card or traditional BNPL).

## 2. PROCESSING DESCRIPTION

To facilitate understanding of the processing activities carried out by Scalapay IP, we set out below a table containing: (i) the categories of personal data processed, (ii) the purposes of processing, (iii) the "legal basis" that authorises each processing activity and renders it lawful, and (iv) the period of time for which Scalapay IP will retain your personal data ("**Personal Data**" or "**Data**").

| **Category of Data** | **Purpose of Processing** | **Legal Basis** | **Retention Period** |
|---|---|---|---|
| Merchant contact and identification data (e.g., first name, last name, business e-mail address and phone number of the Merchant's employees). | - Performance of the contract concluded with the Merchant.<br>- Creation and management of the Merchant's profile on the Scalapay Business Platform. | Performance of a contract to which the Data Subject is party, or execution of pre-contractual measures taken at the Data Subject's request (Article 6, paragraph 1, letter b) of GDPR). | 10 (ten) years from termination of the contractual relationship. |
| Biometric data of the Merchant's authorised representative or legal representative (in particular, derived from the facial characteristics of the authorised representative or legal representative as captured from the selfie or video-selfie taken by the authorised representative or legal representative). | Performing customer due diligence. | Legal obligation to which the Controller is subject and pursuit of a public interest (Article 6, paragraph 1, letter c) and e) of GDPR, as well as Article 9, paragraph 2, letter g) of GDPR, in conjunction with Article 2-sexies of Legislative Decree No. 196/2003) for the purposes of anti-money laundering legislation and fraud prevention, as expressly provided by sector-specific legislation (Legislative Decree No. 231/2007). | 10 (ten) years from completion of the customer due diligence process. |
| Data contained in the identity document of the Merchant's authorised representative or legal representative, as well as a selfie or video selfie taken by them as part of the verification process. | | Legal obligation to which the Controller is subject and pursuit of a public interest (Article 6, paragraph 1, letter c) and e) of GDPR) for the purposes of anti-money laundering legislation and fraud prevention, as expressly provided by | |

| | | | |
|---|---|---|---|
| | | sector-specific legislation (Legislative Decree No. 231/2007). | |
| - Image of the face of the Merchant's authorised representative or legal representative.<br>- Data contained in the identity document. | Performing customer due diligence - through Alternative Verification (as defined and described in Section 4) - by comparing the facial image of the Merchant's authorized representative or legal representative with the facial image depicted in the identity document. | Legal obligation to which the Controller is subject and pursuit of a public interest (Article 6, paragraph 1, letter c) and e) of GDPR) for the purposes of anti-money laundering legislation and fraud prevention, as expressly provided by sector-specific legislation (Legislative Decree No. 231/2007). | 10 (ten) years from completion of the customer due diligence process. |
| Images and videos acquired from the Merchant's authorised representative or legal representative (selfie or video-selfie) and data contained in identity documents. | Carrying out further identity verification checks based on artificial intelligence technologies ("AI") applied to the provided images and videos, to strengthen the verification of correspondence with identity documents and to prevent fraud or misuse of the services. | Legal obligation to which the Controller is subject and pursuit of a public interest (Article 6, paragraph 1, letter c) and e) of GDPR), in conjunction with Legislative Decree No. 196/2003 and Legislative Decree No. 231/2007 (anti-money laundering and fraud prevention legislation). | 10 (ten) years from completion of the customer due diligence process or, in any event, until completion of the verification checks through AI. |
| Identification data contained in the identity document (e.g., first name, last name, date and place of birth, document issue and expiry date), including data collected through automated tools where customer due diligence through biometric identification is unsuccessful. | Where the biometric identification process does not allow certain information contained in the identity document (such as the issue and expiry dates) to be properly captured, such data may be acquired through an automated reading system (OCR – Optical Character Recognition). | Legal obligation to which the Controller is subject and pursuit of a public interest (Article 6, paragraph 1, letter c) and e) of GDPR) for the purposes of anti-money laundering legislation and fraud prevention, as expressly provided by sector-specific legislation (Legislative Decree No. 231/2007). | The data is deleted at the end of the reading process. |
| Identification data contained in the identity document (e.g., first name, last name, date and place of birth, document issue and expiry date, facial image). | Document verification carried out during the customer due diligence process through an AI-based system. Automated analysis of the document image (prior to selfie capture) to verify its authenticity, integrity and the presence of any signs of tampering or forgery, following upload by the Merchant. | Legal obligation to which the Controller is subject and pursuit of a public interest (Article 6, paragraph 1, letter c) and e) of GDPR) for the purposes of anti-money laundering legislation and fraud prevention, as expressly provided by sector-specific legislation (Legislative Decree No. 231/2007). | 10 (ten) years from completion of the customer due diligence process. |
| Identification data of the Merchant's authorised representative or legal representative (first name, last name, date and place of birth, nationality). | Verification of the presence of the Merchant's authorised representative or legal | Legal obligation to which the Controller is subject (Article 6, paragraph 1, letter c) of GDPR) for the | 10 (ten) years from completion of the customer |

| | | | |
|---|---|---|---|
| | representative on lists of politically exposed persons (PEPs) and on international sanctions and embargo lists, in the context of enhanced customer due diligence obligations. | purposes of anti-money laundering and counter-terrorist financing legislation (Legislative Decree No. 231/2007). | due diligence process. |
| Personal data relating to the Merchant's employees and/or collaborators provided spontaneously. | Providing support to the Merchant. | Performance of a contract to which the Data Subject is party, or execution of pre-contractual measures taken at the Data Subject's request (Article 6, paragraph 1, letter b) of GDPR). | For the time necessary to respond to the Data Subject and, in any event, for a period not exceeding 2 (two) years. |
| Identification and personal data of the Merchant as a natural person (tax identification number and VAT number). | Fulfilment of legal obligations regarding electronic transmission to the Italian Revenue Agency. | Legal obligation to which the Controller is subject and the performance of a task carried out in the public interest pursuant to Article 6, paragraph 1, letter c) and e) of GDPR), in conjunction with Article 22, paragraphs 5 and 6, of Decree-Law No. 124/2019, converted into Law No. 157/2019, as well as with the implementing measure of the Italian Revenue Agency and the Implementation Protocol No. 142285/2025. | 10 (ten) years from the date on which the debit was made. |
| Identification and contact data of the Merchant, of its authorised representative and of its legal representative, financial and commercial data provided during onboarding, information on the performance of the business relationship. | Risk assessment for the purposes of deciding whether to proceed with the Merchant's onboarding, and whether to maintain or terminate the business relationship. | Execution of pre-contractual measures taken at the Merchant's request (Article 6, paragraph 1, letter b) of GDPR). | For the duration of the relationship with the Merchant. |

**3. THIRD-PARTY LINKS**

The Scalapay Business Platform does not include links to third-party websites.

**4. IF YOU DO NOT PROVIDE YOUR PERSONAL DATA**

In certain cases, we need to collect your Personal Data by law or under the terms of a contract we have with you or are seeking to enter into with you. In these cases, failure to provide Personal Data will prevent Scalapay IP from entering into a contract with you and/or providing you with the service.

In particular, in order to comply with the sector-specific legislation applicable to the Company, the provision of Data for biometric verification purposes is mandatory to enable us to perform identity verification online. In any event, where the Merchant's legal representative or authorised representative is unable, due to technical limitations of their device, to proceed with online identity verification, or has exhausted the identity verification attempts offered by the Company, the Merchant's legal representative or authorised representative may send an e-mail to support@scalapay.com attaching (i) a photograph of a valid identity document (or equivalent document) and (ii) a photograph showing the face of the

Merchant's legal representative or authorised representative and the identity document held in hand. The Company's staff will perform the identity verification manually ("**Alternative Verification**"). In that case, no biometric data of the Merchant's legal representative or authorised representative will be processed.

**5. INTERNATIONAL TRANSFERS**

Some of our suppliers are located outside the European Union. When we transfer your Data to these suppliers, we ensure that your Data are processed in a manner substantially equivalent to the level of protection applicable within the European Union. In this regard, in compliance with the safeguards provided for under the GDPR, your data are transferred on the basis of:

- adequacy decisions: where the transfer of personal data takes place to countries that have been deemed by the European Commission to provide an adequate level of protection for personal data;
- standard contractual clauses: in the absence of adequacy decisions, we will use specific contracts approved by the European Commission, designed to guarantee the same level of personal data protection applicable within the European territory.

The list of countries outside the European Union to which Scalapay IP may transfer your Data (including information on the safeguards adopted) is available upon request by contacting us at the details indicated in this notice.

**6. TO WHOM WE MAY DISCLOSE YOUR PERSONAL DATA?**

Within the organisation of Scalapay IP, Data may be processed by the employees of the competent departments responsible for carrying out the individual processing activities.

Furthermore, in order to provide our services, we may disclose your Personal Data to the categories of recipients listed below, for the purposes set out herein, in compliance with the principles of minimisation and purpose limitation, and with the implementation of appropriate security measures. In particular, for the provision of services, the categories of parties to whom we will disclose Data, within the scope and limits of the purposes pursued, are:

- Suppliers: we may disclose Personal Data to suppliers, with whom we enter into contractual agreements, that we use to provide you with services. Examples include software and data storage providers, payment processing services, and business consultants.

- Scalapay S.r.l.: Scalapay IP may disclose your personal data to Scalapay S.r.l., which develops and manages the Scalapay Business Platform, acting as data processor on behalf of Scalapay IP.

- KYC (Know-Your-Customer)/AML (Anti-Money Laundering) agencies: in the context of Merchant onboarding operations, identity checks are performed on the company and its beneficial owner.

- Debt collection companies and/or law firms: Scalapay IP may need to share your Data for the purpose of carrying out recovery of overdue and unpaid receivables.

- Authorities: Scalapay IP may provide information deemed necessary to police, financial, tax or other authorities and courts, including the Bank of Italy or the Revenue Agency. Personal Data are shared with the authority where required by law, in certain cases at your request, or for the combating of crime. An example of a legal obligation to provide information arises where it is necessary to take measures against money laundering and terrorist financing.

Such entities will have access to the Personal Data necessary to perform the functions governed by an agreement between the companies and will act, depending on the circumstances, as independent data controllers or data processors (in the latter case, pursuant to a data processing agreement under Article 28 GDPR).

**7. FOR HOW MUCH WE WILL USE YOUR PERSONAL DATA?**

Further information on the retention period for your personal data can be found in the table in Section 2. We retain your Data only for as long as necessary to achieve the purposes for which they were collected, such as the performance of the contract or the fulfilment of legal obligations. When deciding how long to retain your Data, we take into account the quantity and type of Data, their sensitivity and the risk of misuse. After this period, your data will be deleted or anonymised.

**8. BIOMETRIC VERIFICATION PROCESSING. ABSENCE OF AUTOMATED DECISION-MAKING**

The Company uses biometric technologies to perform identity verification of the authorised representatives or legal representatives connected to the Merchant who intend to enter into a contract with Scalapay IP. As indicated in Section 2, this processing is carried out to comply with legal obligations in the area of prevention of money laundering and terrorist financing, as required by anti-money laundering legislation (i.e. Legislative Decree No. 231/2007).

Outside the scope of Alternative Verification (which, as indicated in Section 4, applies exclusively in residual cases), the identity verification process is carried out through facial verification technologies based on a one-to-one comparison (between the facial image captured by the selfie or video and that present in the identity document provided). To carry out this verification, we will ask the Merchant's authorised representative or legal representative to:

- upload a photograph of the identity document (or equivalent document) directly to the Scalapay Platform;
- take a selfie or record a short video using the device's camera, following specific instructions that ensure correct image capture (e.g., adequate lighting conditions and the absence of other people in the frame).

We will screen the biometric data of the Merchant's authorised representative or legal representative (the selfie or video referred to above) to verify the correspondence of the face with the photograph in the relevant identity document, verifying the consistency of the information contained in the identity document with that provided, as well as the framing and environmental conditions. The Merchant's authorised representative or legal representative who undergoes biometric verification will always be aware of the collection of biometric data. Furthermore, Scalapay IP will never, through the process just described, make decisions based solely on automated processing that produce legal effects or similarly significantly affect the Merchant. Indeed, where the verification is unsuccessful, the Company's staff will always be involved to assess the reasons.

For further information on the type of technology used by the Company and, in any event, to exercise such rights, please contact our Data Protection Officer (DPO) at the addresses indicated below.

Where automated tools are used for the extraction of data from identity documents, such systems do not autonomously determine the outcome of the verification process, but exclusively support the identification activity, which is completed by authorised personnel or through further controls.

Identity verification procedures also include a check on the reliability of the image of the document provided, both through a comparison of the video and facial images acquired during the identification process with the images present in the document, and through analysis of the elements that make an identity document reliable. These checks are carried out through an AI system, which does not acquire additional data or store information contained in documents. In addition to complying with regulatory obligations regarding the correct identification of the data subject, the checks are intended to prevent possible fraud, for the better protection of services and customers themselves. The AI technologies employed operate in compliance with the principles of lawfulness, fairness, transparency, proportionality and data minimisation, and do not lead to decisions based solely on automated processing that produce legal effects or significantly affect the data subject.

**9. YOUR RIGHTS**

Please note that you may exercise your rights relating to personal data in the manner and within the limits provided for by data protection legislation. Below is a brief description of such rights:

- **Right to be informed**: all natural persons have the right to be informed about the collection and use of their Personal Data. This is a fundamental transparency requirement as established by the GDPR. This Notice and the responses we provide to your requests satisfy this requirement.

- **Right to request access to Personal Data**: known as a "subject access request", this enables you to obtain confirmation as to whether or not processing of Data is taking place and, where it is, to obtain access to the Data and information referred to in the GDPR, as well as to obtain a copy of your Personal Data.

- **Right to request rectification of personal data**: this enables you to correct and supplement any incomplete or inaccurate Data in our possession; however, we may need to verify the accuracy of the new data provided.

- **Right to request erasure of personal data ("right to be forgotten")**: this enables you to request the removal and erasure of your Personal Data where there are no valid grounds for continuing to process them. Erasure of your Personal Data may be obtained in the cases provided for in Article 17 GDPR. However, please note that in certain cases we may be unable to fulfil your erasure request for specific legal reasons (e.g., where erasure is necessary to enable you to comply with a legal obligation or to establish, exercise or defend a right in legal proceedings), which will be communicated to you at the time of your request.

- **Right to object to the processing of personal data**: as provided for in Article 21 GDPR, you may object to the processing of Data, on grounds relating to your particular situation, in cases where we, or a third party, rely on legitimate interests and you consider that such processing adversely affects in some way your fundamental rights and freedoms. In that case, the Company will cease to process the Personal Data further unless the Company demonstrates the existence of compelling legitimate grounds for the processing that override your interests, rights and freedoms, or for the establishment, exercise or defence of a right in legal proceedings.

- **Right to request restriction of processing of personal data**: you may request restriction of the processing of your Personal Data in the cases provided for in Article 18 GDPR; we will continue to process personal data only where an exception to such request applies (e.g., where processing is unlawful and you oppose erasure of the Data, requesting instead that its use be restricted).
- **Right to request transfer of personal data to you or to a third party ("data portability")**: we will deliver to you or to a party designated by you your Personal Data in a structured, commonly used and machine-readable format, under the conditions provided for in Article 20 GDPR. Please note that this right applies only to information processed by automated means and to processing carried out on the basis of consent, or in the context of the performance of a contract concluded with you.

- **Right to withdraw consent at any time**: with regard to any processing based on your consent (as collected from time to time by Scalapay IP following provision of an appropriate notice), you will have the right to withdraw at any time the consent given for the processing of Personal Data based on consent, and we will cease to use your personal data, without, however, affecting the lawfulness of processing based on consent before its withdrawal.

- **Right to lodge a complaint with a supervisory authority**: please note that you always have the right to lodge a complaint with the Italian Data Protection Authority (Garante per la Protezione dei Dati Personali), with offices at Piazza Venezia 11, Rome, at the e-mail address: protocollo@gpdp.it.

## 10. COOKIES

Scalapay IP does not use any type of cookie. This means that when you browse our website (at https://paymentinstitute.scalapay.com/), we do not collect information about your device, such as browsing data or preferences. We do not use third-party cookies for tracking or personalised advertising, and we do not share your information with third parties through the use of cookies.

## 11. CHANGES TO THIS NOTICE

We reserve the right to amend this notice at any time, including to adapt it to legislative or regulatory changes. In the event of material changes, we will inform you with reasonable notice, through the Scalapay Platform or another appropriate channel, before they take effect. We invite you to consult this page periodically to stay up to date.

## 12. CONTACTS

To exercise your rights or to request information about how we process your Personal Data, you may contact us by e-mail scalapayip@legalmail.it and we will do our utmost to assist you.

Furthermore, if you have questions relating to the processing of personal data, including requests to exercise your rights, you may also contact our DPO at the following e-mail address: privacy@ip.scalapay.com.