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.

* * *

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). 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.

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
Consumer contact and identification data, 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, e-mail address, mobile phone number, nationality, identity document (type, number, date of issue, issuing authority, city). Details relating to goods/services purchased or ordered, such as the type of item and the type of Merchant at which purchases are made.	Provision of payment services to Consumers (Pay in 3, Pay in 4, Pay Later or virtual payment card) and the following activities: – Sending e-mails relating to the transaction; – Transfer of information to the Merchant for performance of the contract; – Providing support upon Consumer request.	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).	
Image of the Data Subject'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	Legal obligation to which the Controller is subject and pursuit of a public interest (Article 6, paragraph 1, letter c) and	10 (ten) years from completion of the customer due diligence process.

Category of Personal Data	Purpose of Processing	Legal Basis	Retention Period
	image depicted in the identity document.	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).	
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.
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.

Category of Personal Data	Purpose of Processing	Legal Basis	Retention Period
	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.
Data provided spontaneously by the Consumer.	Providing responses to Consumer requests (e.g., in the case of a request for support in completing the due diligence 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 time necessary to respond to the Consumer and, in any event, for a period not exceeding 2 (two) years.
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.
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. For these purposes, Scalapay IP may: - consult Credit Information Systems ("CIS"), such as CRIF S.p.A.; - communicate to such CIS information relating to the request for the use of the services, the outcome of such request and the payment performance.	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). 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 the terms and conditions set out in the Code of Conduct for CIS and applicable legislation.

Category of Personal Data	Purpose of Processing	Legal Basis	Retention Period
Data relating to the Consumer's employment and financial situation, collected in the context of a request to use the Pay in 6, 9, 12 service. 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 6, 9, 12 service, for the purpose of determining whether the transaction may be approved, prior to any consultation of Credit Information Systems (CIS).	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.
Identification data in pseudonymised format. 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: - accurate assessment of the creditworthiness and credit risk of Consumers requesting one of the payment instruments offered by the Controller; - proper evaluation of the reliability and timeliness of Consumers' payments; - 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.	60 (sixty) days from the risk analysis.

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 6, 9, 12 service, 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) 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 Pay in 6, 9, 12 service.

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. as the operator of the Scalapay Platform on which you have created a user profile.

- 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.

- Credit Information Systems (**CIS**): Scalapay IP may disclose the Consumer's Personal Data to CIS, such as CRIF S.p.A., for the purpose of assessing creditworthiness, preventing fraud and managing credit risk. These entities act as independent data controllers.

- 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")

Where the Consumer requests the use of one of the instalment payment services offered by Scalapay IP, including Pay in 6, 9, 12 service, the Controller may consult one or more CIS, such as, by way of example, CRIF S.p.A., for the purpose of assessing the Consumer's creditworthiness and reliability.
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 6, 9, 12 service 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 the Code of Conduct for Credit Information Systems and applicable legislation.

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, for CRIF S.p.A., on its institutional website).

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 9 (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 6, 9, 12 service, 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.

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 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. 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; - 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 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. - 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.	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.
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	For the time necessary to respond to the Data Subject and,

		taken at the Data Subject's request (Article 6, paragraph 1, letter b) of GDPR)	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.

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. as the operator of the Scalapay Business Platform on which you have created a profile.

- 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. 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.