SCALAPAY IP S.P.A. - PRIVACY POLICY

Scalapay IP S.p.A., a payment institution established under the Italian law, with registered office at Via Nervesa, 21, 20139 Milan (MI), C.F. and P. IVA 06078740484, which carries out its activities pursuant to Art. *114-sexies* et seq. of Legislative Decree No. 385 of September 1, 1993 ("**TUB**"), registered under no. 36018.0 of the Register of Payment Institutions pursuant to Article *114-septies* of the TUB and subject to the supervision of the Bank of Italy (hereinafter also "**Scalapay IP**" or "**Data Controller**" or "**Company**"), as the data controller, respects your privacy and is committed to protecting your personal data. Scalapay IP is committed to processing your data in accordance with the General Data Protection Regulation (EU Reg. 2016/679), better known as "**GDPR**", and any other applicable privacy laws.

This policy explains the reasons, how personal data is collected, managed and protected in relation to **customers of Scalapay IP's services, also referred to below as Consumers (SECTION A)** as well as **Scalapay IP's affiliated dealers, also referred to below as Merchants (SECTION B)**.

In particular, the processing of personal data carried out by Scalapay IP will be based on the principles of lawfulness, fairness, transparency, purpose limitation and storage, data minimization, accuracy, integrity and confidentiality.

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

It is important that you read this policy, along with any other notices we may provide to supplement, update, or expand on information regarding the collection and processing of your personal information. We will try to coordinate these disclosures so that at all times we represent the conditions applied to the processing of your personal data in the most transparent and easily accessible way.

* * *

SECTION A - CONSUMER PRIVACY POLICY

1. DATA CONTROLLER

This policy is drafted pursuant to Articles 13 and 14 of the GDPR and is intended to provide you with information on how Scalapay IP processes your personal data as a data controller. Your personal data is collected through your 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**") can purchase products and services of affiliated dealers (hereinafter, the "**Merchants**") through one of the payment services (e.g. Pay *in 3, Pay in 4, Pay Later, One Time Card* or *Pay Now-Cart Saver* via one time card or traditional BNPL) offered by Scalapay IP. For the purpose of executing the contract concluded with the Merchant, Scalapay IP also processes Data collected by the Merchants and/or Scalapay S.r.l..

2. DESCRIPTION OF THE PROCESSING

To facilitate the understanding of the processing activities put in place by Scalapay IP, we provide below a table containing the categories of personal data processed, the purposes of the processing, the "legal basis" that authorizes each processing and ensures its lawfulness as well as the period of time for which Scalapay IP will retain your personal data ("**Personal Data**" or "**Data**").

Data Category	**Purpose of processing**	**Legal Basis**	**Retention period**
Consumer contact and identification data, goods/service data, and payment data . For example, first name, last name, social security number, residential address (state, province, city, ZIP code), shipping address, place of birth, date of birth, gender, e-mail address, cell phone number, nationality, ID (type, number, date of issue, issuing authority, city) Details about the goods/services purchased or ordered, such as the type of item and the type of Merchant you shop on	Provision of payment services to Consumers (Pay *in 3*, Pay in 4, *Pay later* or virtual payment card) and in particular provision of the following activities: - Sending emails related to the transaction - Transfer of information to the Merchant for contract performance - Provide support in the event of a request from the Consumer	Performance of a contract to which the Consumer is a party or in order to take steps at the request of the data subject prior to entering into a contract (Article 6(1)(b) of the GDPR)	10 (ten) years after the termination of the contract
Biometric data of the Consumer (specifically, from the features of the Consumer's face taken from the selfie taken by the Consumer or the video selfie taken by the Consumer)	Conduct customer due diligence by biometric identification of the Consumer's face	Legal obligation to which the Data Controller is subject and the pursuit of a public interest (Article 6(1)(c) and (e) of the GDPR and Article 9(2)(g) of the GDPR, read in conjunction with Article *2sexies* of Legislative Decree 196/2003) for the purposes of anti-money laundering legislation and to prevent fraud, as expressly provided for in the relevant legislation (Legislative Decree 231/2007)	10 (ten) years after the conclusion of the due diligence process
Data contained in the Consumer's ID and selfie or video selfie taken by the Consumer as part of the verification		Legal obligation to which the Data Controller is subject and the pursuit of a public interest (Article 6(1)(c) and (e) of the GDPR) for the purposes of anti-money laundering regulations and to prevent fraud, as expressly provided for in the relevant legislation (Legislative Decree 231/2007)	
Image of the face of the Data Subject, Data contained in the identity document	Perform customer due diligence - via Alternative Verification (as defined and described in Section 4) - by making a comparison between the image of the Consumer's face and the image of the face portrayed in the identity document	Legal obligation to which the Data Controller is subject and the pursuit of a public interest (Article 6(1)(c) and (e) of the GDPR) for the purposes of anti-money laundering regulations and to	10 (ten) years after the conclusion of the due diligence process

Data Category	Purpose of processing	Legal Basis	Retention period
		prevent fraud, as expressly provided for in the relevant legislation (Legislative Decree 231/2007)	
Identifying data on the ID document (e.g., first name, last name, date and place of birth, date of issuance and expiration of the document), including collected through automated means in case of failure of customer due diligence by biometric identification	In the event that the customer due diligence by biometric identification cannot correctly capture some information from the ID document (e.g., issuance and expiration dates), such data may be captured by an automated reading system (OCR - Optical Character Recognition)	Legal obligation to which the Data Controller is subject and the pursuit of a public interest (Article 6(1)(c) and (e) of the GDPR) for the purposes of anti-money laundering regulations and to prevent fraud, as expressly provided for in the relevant legislation (Legislative Decree 231/2007)	The data is deleted at the end of the reading process
Financial and payment-related data (e.g., last four digits of card, expiration date and place of issuance, IBAN)	Process order payment and manage collections and payments	Performance of a contract to which the Consumer is a party or in order to take steps at the request of the data subject prior to entering into a contract (Article 6(1)(b) of the GDPR)	10 (ten) years after the termination of the contract
	AUI (Archivio Unico Informatico) management, particularly reports carried out to fulfill regulatory and reporting obligations to the Bank of Italy	Legal obligation to which the Data Controller is subject (Article 6(1)(c) of the GDPR)	10 (ten) years after the entry of the report
Data voluntarily provided by the Consumer	Provide feedback to Consumer requests (e.g., in the case of a request for support to conduct due diligence)	Performance of a contract to which the Consumer is a party or in order to take steps at the request of the data subject prior to entering into a contract (Article 6(1)(b) of the GDPR)	For the time necessary to provide feedback to the Consumer and, in any case, for a period not exceeding 2 (two) years
All Personal Data shown in this table (except biometric data).	Management of any disputes with Consumers	Pursuit of the legitimate interest of the Data Controller in establishing, exercising or defending a right in judicial proceedings or whenever judicial authorities exercise their judicial functions (Article 6(1)(f))	Until the conclusion of the dispute
Identification data in pseudonymised format Personal Data relating to transactions already carried out using the Data Controller	Analysis of the integration of Scalapay IP technology with third-party components to achieve the following objectives: - correct measurement of the creditworthiness and credit risk	Scalapay IP processes personal data on the basis of its legitimate interest (Art. 6(1)(f) GDPR). This processing is necessary to ensure	60 days after risk analysis

Data Category	Purpose of processing	Legal Basis	Retention period
services (transaction amounts, transaction dates and instalment due dates, payment status)	of Consumers requesting one of the Data Controller's payment instruments - correct assessment of the reliability and punctuality of the Consumers' payments - prevention of the risk of fraud, including prevention of the risk of identity theft	responsible risk management, prevent fraud and protect consumers from excessive debt. The processing has been subject to a balancing of interests to ensure that it does not undermine 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	

3. THIRD-PARTY LINKS

The Scalapay Platform, which you access in order to make deferred purchases from Merchants, may include links to third party websites (such as the websites of the stores on which you purchase products or services). Clicking on or enabling such links may allow third parties to process your Personal Data; therefore, we encourage you to also refer to the privacy policy of those sites, as well as the Scalapay Platform's privacy policy.

4. IF YOU DO NOT PROVIDE YOUR PERSONAL INFORMATION

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

More specifically, in order to comply with industry regulations applicable to the Company, the provision of Data for biometric verification purposes is mandatory to enable us to perform *online* identity verification. In any case, where the Consumer is unable due to technical limitations of the device to proceed with the verification of his or her identity online, or has exhausted the identity verification attempts made available by the Company, the Consumer may send an email to support@scalapay.com attaching (i) a photo of a valid identity document (or other equivalent document) and (ii) a photo in which the Consumer's face and the identity document held in his or her hand are visible. It will be the responsibility of the Company's personnel to manually perform the identity verification ("**Alternative Verification**"). In such case, no biometric data of the Consumer 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 is processed and protected in substantially the same way as it would be in the EU. In this regard, subject to the safeguards in the GDPR, your Data is transferred on the basis of:

- adequacy decisions: when personal data is transferred to countries that have been deemed to provide an adequate level of personal data protection by the European Commission;
- standard contract clauses: in the absence of adequacy decisions, we will use specific contracts approved by the European Commission, aimed at ensuring the same protection of personal data provided within the European territory.

A list of countries outside the European Union to which Scalapay IP may transfer your data (including information about the safeguards in place) is available upon request by contacting us at the contact information provided in this policy.

6. TO WHOM CAN WE DISCLOSE YOUR PERSONAL INFORMATION?

Within the organization of Scalapay IP, the Data may be processed by the persons in charge of the offices responsible for carrying out individual processing activities.

In addition, in order to provide our services, we may disclose your Personal Data to the categories of recipients listed below, for the purposes listed below, in accordance with the principles of minimization and purpose limitation, taking 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 the services, the categories of subjects to whom we will communicate Data, by reason of and within the limits of the purposes pursued, are:

- Providers: we may disclose Personal Data to providers - with whom we enter into contractual arrangements - that we use to provide services to you. Examples of such suppliers include software and data storage providers, payment processing services, business consultants, companies that provide biometric face scanning software to Consumers, and *affiliate network* companies.

- Augusta SPV S.r.l.: Scalapay IP may disclose your Personal Data to the company Augusta SPV s.r.l., a credit securitization vehicle pursuant to l. April 30, 1999 No. 130, as it is involved in the securitization 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 owner of the Scalapay Platform at which you have created a user profile.

- Online and physical stores: Scalapay IP may disclose Personal Data to the online store from which you make a purchase. This is done in order for the store to administer your purchase and your relationship with the store, send you products, handle any disputes, and prevent fraud. Personal information disclosed to a store will be subject to the store's privacy policy.

- Payment service providers ("**PSPs**"): PSPs allow you to accept electronic payments through a wide range of payment methods, such as credit card, bank payments such as direct debit, etc.

- Debt Collection Companies: Scalapay IP may need to share your Data when selling or outsourcing the collection of overdue and unpaid debts to a third party, such as a debt collection company.

- Companies that assess consumers' creditworthiness: In order to ensure proper credit assessment and transaction security, Scalapay IP may share certain data with third party partners, including the company Qlarifi Limited. The data shared may include information on transactions made, consumer identification data and payment history. Qlarifi processes this data solely for scoring and fraud prevention purposes, in accordance with existing data processing agreements.

- Authorities: Scalapay IP may provide information deemed necessary to law enforcement, financial, tax or other authorities and courts, including the Bank of Italy or Internal Revenue Service. Personal Data is shared with the authority if required by law, in some cases at your request, or if necessary for the administration of tax deductions, to combat crime, or to protect our rights in judicial or extra-judicial proceedings. An example of a legal obligation to provide information is when it is necessary to take measures against money laundering and terrorist financing.

These individuals will have access to the Personal Data necessary to perform the functions governed by an agreement between the companies, and will act - as the case may be - as autonomous data controllers or data processors (in the latter case, by virtue of an agreement to be appointed as a controller under Article 28 GDPR).

7. HOW LONG WILL WE USE YOUR DATA?

You can find more information about the retention period in the chart in Section 2. We only keep your Data for as long as necessary to achieve the purposes for which we collected it, such as performing the contract or fulfilling legal obligations.

When we decide how long to keep your Data, we consider the amount and type of Data, its sensitivity, and the risk of misuse.

At the end of the retention period, the Personal Data will be deleted or anonymized. Therefore, at the expiration of this period, the data subject may not be able to exercise the rights set forth in Section 9 (such as the right to access, erasure, rectification and the right to portability of Personal Data).

8. 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 stated in Section 2, such processing is carried out to comply with legal obligations regarding the prevention of money laundering and the financing of terrorism, as required by anti-money laundering regulations (including Legislative Decree 231/2007).

Outside of the Alternative Verification scenario (which, as stated in Section 4, only finds application in residual cases), the identity verification process is carried out through facial verification technologies that are based on a *one-to-one* comparison (between the image of your face captured by the selfie or video and the one in the ID you provide). In order to perform such verification, we will ask you to:

- Upload a photograph of your ID (or other equivalent document) directly to the Scalapay Platform;
- take a selfie or record a short video via your device's camera, following specific instructions that ensure that the image is captured correctly (e.g., proper lighting conditions and no other people in the frame);

We will perform a screening of your biometric data (the selfie or video aforementioned) to verify that your face matches the photograph in the relevant ID document, checking the consistency of the information included in the ID document with the information you provided, as well as the framing and environmental conditions. You will still be aware of the collection of the biometric data. But that's not all: Scalapay IP will never - through the process just described - make decisions based solely on automated processing that produce legal effects or significantly affect you in a similar way. In fact, should the verification fail, the Company's staff will always be involved to assess the reasons why.

For more information about the type of technology used by the Company and, in any case, to exercise these rights, you can contact our Data Protection Officer (DPO) at the addresses listed below.

In the case of using automated tools to extract data from identity documents, such systems do not independently determine the outcome of the verification process, but only support the identification activity, which is completed by authorized personnel or additional checks.

9. YOUR RIGHTS

We remind you that you can exercise your rights regarding personal data in the manner and within the limits provided by data protection laws. Below is a brief description of these rights that you can exercise when the conditions provided by the GDPR are met:

- **Right to be informed**: all individuals have the right to be informed about the collection and use of their Personal Data. This is a fundamental requirement of transparency as set forth in the GDPR. This Policy and the responses we will provide to your inquiries fulfill this requirement.

- **Right to Request Access to Personal Data**: known as an "access request," allows you to obtain confirmation of whether or not Data is being processed and if so, to obtain access to the Data and information mentioned by the GDPR, as well as to obtain a copy of your Personal Data.

- **Right to Request Rectification of Personal Data**: allows you to correct and supplement any incomplete or inaccurate Data we hold; however, we may need to verify the accuracy of the new data provided.

- **Right to request deletion of Personal Data ("right to be forgotten")**: allows you to request the removal and deletion of your Personal Data where there are no valid reasons to continue processing it. You can obtain the deletion of your Personal Data in the cases listed in Article 17 GDPR. However, please note that in certain circumstances we may not be able to comply with your request for deletion for specific legal reasons (e.g., where it is necessary to enable you to comply with a legal obligation or to establish, exercise or defend a right in court) that will be communicated to you at the time of your request.

- **Right to object to the processing of Personal Data**: under the terms of Article 21 GDPR, you may object to the processing of the Data, on grounds related to your particular situation, in cases where we, or a third party, should rely on legitimate interest and should you believe that such processing in any way infringes upon your fundamental rights and freedoms. In which case, the Company will refrain from further processing Personal Data unless the Company demonstrates the existence of compelling legitimate grounds for processing that override your interests, rights and freedoms or for the establishment, exercise or defense of a legal claim. To exercise this right, you can contact us at privacy@ip.scalapay.com.

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

- **Right to request the transfer of Personal Data to you or a third party ("data portability")**: we will deliver your Personal Data to you or to a party delegated by you in a structured, commonly used and machine-readable format, under the conditions set out in Article 20 GDPR. Please note that this right applies only to information processed by automated means and for processing that takes place on the basis of consent, or as part of the fulfillment of the contract entered into with you.

- **Right to Revoke Consent at Any Time**: Limited to any processing based on your consent (as collected from time to time by Scalapay IP following the provision of appropriate notice) you will have the right to revoke your consent given for consent-based processing of Personal Data at any time and we will cease to use your Personal Data, but without affecting the lawfulness of the processing based on the consent given prior to revocation.

- **Right to file a complaint with the authority**: we remind you that you always have the right to file a complaint with the Italian Data Protection Authority, based at Piazza Venezia 11, Rome, at the e-mail address: protocollo@gpdp.it.

10. COOKIE

Scalapay IP does not use any type of cookies on its institutional site (https://paymentinstitute.scalapay.com/). This means that while you are browsing our site, we do not collect any information on your device, such as browsing data or preferences. We do not use third-party cookies for tracking or personalized 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 can contact us by e-mail at scalapayip@legalmail.it and we will do what we can to help you.

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

* * *

SECTION B - MERCHANT PRIVACY POLICY

1. DATA CONTROLLER

This policy is prepared in accordance with Articles 13 and 14 of the GDPR and is intended to provide you with information on how Scalapay IP processes your personal data. Your personal data has been collected by Scalapay S.r.l. through your use of the website www.scalapay.com and the business platform (hereafter, the "**Scalapay Business Platform**") or by Scalapay IP when you sign a contract with Scalapay IP as an affiliate merchant (hereafter, also "**Merchant**") in order to offer your customers one of the payment services (e.g. *Pay in 3*, *Pay in 4, Pay Later, One Time Card* or *Pay Now-Cart Saver* via one time card or traditional BNPL) offered by Scalapay IP.

2. DESCRIPTION OF THE PROCESSING

To facilitate the understanding of the processing activities put in place by Scalapay IP, we provide below a chart containing the categories of personal data processed, the purposes of the processing, the "legal basis" that authorizes each processing and gives it lawfulness as well as the period of time for which Scalapay IP will retain your personal data ("**Personal Data**" or "**Data**").

Data category	**Purpose of processing**	**Legal Basis**	**Retention period**
Merchant's contact and identification data (e.g., first name, last name, e-mail address, and business phone number of Merchant's employees)	- Execution of the contract signed with the Merchant - Creating and managing the Merchant profile on the Scalapay Business Platform.	Performance of a contract to which the Consumer is a party or in order to take steps at the request of the data subject prior to entering into a contract (Article 6(1)(b) of the GDPR)	For 10 (ten) years after the termination of the contractual relationship
Biometric data of the executor or legal representative of the Merchant (in particular, starting from the facial features of the executor or legal representative taken from the selfie taken by the executor or legal representative or from the video-selfie made by them).	Conduct Merchant due diligence	Legal obligation to which the Data Controller is subject and the pursuit of a public interest (Article 6(1)(c) and (e) of the GDPR and Article 9(2)(g) of the GDPR, read in conjunction with Article *2 sexies* of Legislative Decree 196/2003) for the purposes of anti-money laundering legislation and to prevent fraud, as expressly provided for in the relevant legislation (Legislative Decree 231/2007)	10 (ten) years after the conclusion of the due diligence process
Data contained in the identity document of the executor or legal representative of the Merchant and selfies or video selfies taken by them as part of the due diligence.		Legal obligation to which the Data Controller is subject and the pursuit of a public interest (Article 6(1)(c) and (e) of the GDPR) for the purposes of anti-money laundering regulations and to prevent fraud, as expressly provided for in the relevant legislation (Legislative Decree 231/2007)	

-Image of the face of the executor or legal representative of the Merchant -Data contained in the identity document of the executor or legal representative of the Merchant	Conduct Merchant due diligence – through Alternative Verification (as defined and described in Section 4) – by comparing the facial image of the Merchant's executor or legal representative with the facial image in the identity document	Legal obligation to which the Data Controller is subject and the pursuit of a public interest (Article 6(1)(c) and (e) of the GDPR) for the purposes of anti-money laundering regulations and to prevent fraud, as expressly provided for in the relevant legislation (Legislative Decree 231/2007)	10 (ten) years after the conclusion of the due diligence process
Identifying data on the ID document of the executor or legal representative of the Merchant (e.g., first name, last name, date and place of birth, date of issuance and expiration of the document), including collected through automated means in case of failure of Merchant due diligence by biometric identification	In the event that the Merchant due diligence by biometric identification cannot correctly capture some information from the ID document (e.g., issuance and expiration dates), such data may be captured by an automated reading system (OCR - Optical Character Recognition)	Legal obligation to which the Data Controller is subject and the pursuit of a public interest (Article 6(1)(c) and (e) of the GDPR) for the purposes of anti-money laundering regulations and to prevent fraud, as expressly provided for in the relevant legislation (Legislative Decree 231/2007)	The data is deleted at the end of the reading process
Personal data related to employees and/or contractors of the Merchant provided voluntarily	Providing support to the Merchant	Performance of a contract to which the Consumer is a party or in order to take steps at the request of the data subject prior to entering into a contract (Article 6(1)(b) of the GDPR)	For the time necessary to provide feedback to the Interested Party and, in any case, for a period not exceeding 2 (two) years

3. THIRD-PARTY LINKS

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

4. IF YOU DO NOT PROVIDE YOUR PERSONAL INFORMATION

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

More specifically, in order to comply with the industry regulations applicable to the Company, the provision of Data for biometric verification purposes is mandatory to enable us to carry out online identity verification. In any case, where the Merchant's legal representative or executor is unable to proceed with online identity verification due to technical limitations of the device, or has exhausted the identity verification attempts made available by the Company, the Merchant's legal representative or executor may send an email to support@scalapay.com attaching (i) a photo of a valid identity document (or other equivalent document) and (ii) a photo showing the face of the Merchant's legal representative or executor and the identity document held in their hand. The Company's staff will manually verify the identity ("**Alternative Verification**"). In this case, no biometric data of the Merchant's legal representative or executor 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 is processed and protected in substantially the same way as it would be it would be in the EU. In this regard, subject to the safeguards in the GDPR, your Data is transferred on the basis of:

- adequacy decisions: when personal data is transferred to countries that have been deemed to provide an adequate level of personal data protection by the European Commission;

- standard contract clauses: in the absence of adequacy decisions, we will use specific contracts approved by the European Commission, aimed at ensuring the same protection of personal data provided within the European territory.

A list of countries outside the European Union to which Scalapay IP may transfer your data (including information about the safeguards in place) is available upon request by contacting us at the contact information provided in this policy.

6. TO WHOM CAN WE DISCLOSE YOUR PERSONAL INFORMATION?

As part of the Scalapay IP organization, the Data may be processed by the persons in charge of the offices responsible for carrying out individual processing activities.

In addition, in order to provide our services, we may disclose your Personal Data to the categories of recipients listed below, for the purposes listed below, in accordance with the principles of minimization and purpose limitation, taking appropriate security measures. In particular, for the provision of services, the categories of parties to whom we will disclose Data, by reason of and within the limits of the purposes pursued, are:

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

- Scalapay S.r.l.: Scalapay IP may disclose your personal information to Scalapay S.r.l. as the owner of the Scalapay Business Platform at which you created a profile.

- KYC (*Know-Your-Customer*)/AML (*Anti-Money Laundering*) Agencies: as part of the Merchant's "*onboarding*" operations, checks are conducted on the identity of the company and on the beneficial owner.

- Debt collection companies and/or law firms: Scalapay IP may need to share your Data in order to put in place a collection activity for overdue and unpaid debts.

- Authorities: Scalapay IP may provide information deemed necessary to law enforcement, financial, tax, or other authorities and courts, including the Bank of Italy or Internal Revenue Service. Personal information is shared with the authority if required by law, in some cases at your request, or for law enforcement purposes. An example of a legal obligation to provide information is when it is necessary to take measures against money laundering and terrorist financing.

These individuals will have access to the Personal Data necessary to perform the functions governed by an agreement between the companies, and will act - as the case may be - as autonomous data controllers or data processors (in the latter case, by virtue of an agreement to be appointed as a controller under Article 28 GDPR).

7. HOW LONG WILL WE USE YOUR DATA?

You can find more information about the retention period in the chart in section 2. We retain your Data only for as long as necessary to achieve the purposes for which we collected it, such as performing the contract or fulfilling legal obligations. When we decide how long to keep your Data, we consider the amount and type of Data, its sensitivity, and the risk of misuse. After this period, your Data will be deleted or anonymized.

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

The Company uses biometric technologies to verify the identity of the executors or legal representatives linked to the Merchant who wish to enter into a contract with Scalapay IP. As stated in Section 2, this processing is carried out to comply with legal obligations regarding the prevention of money laundering and terrorism financing, as required by anti-money laundering regulations (including Legislative Decree 231/2007).

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

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

We will perform a screening of the biometric data of the executor or legal representative of the Merchant (the selfie or video mentioned above) to verify the correspondence of the face with the photograph of the relative identity document, verifying the consistency of the information included in the identity document with that to be provided, as well as the framing and environmental conditions. The executor or legal representative of the Merchant who will carry out the biometric verification will always be aware of the collection of biometric data. In addition to the above Scalapay IP will never make decisions based solely on automated processing that produces legal effects or significantly affects the Merchant in a similar way through the process just described. In fact, should the verification not be successful, the Company's staff will always be involved to evaluate the reasons.

For more information on the type of technology used by the Company and, in any case, to exercise these rights, you can contact our Data Protection Officer (DPO) at the addresses below.

In the case of using automated tools to extract data from identity documents, such systems do not independently determine the outcome of the verification process, but only support the identification activity, which is completed by authorized personnel or additional checks.

9. YOUR RIGHTS.

Please note that you can exercise your rights regarding your personal data in the manner and within the limits provided by data protection laws. Below is a brief description of these rights:

- **Right to be informed**: all individuals have the right to be informed about the collection and use of their Personal Data. This is a fundamental requirement of transparency as set forth in the GDPR. This Policy and the responses we will provide to your inquiries fulfill this requirement.

- **Right to Request Access to Personal Data**: known as an "access request," allows you to obtain confirmation of whether or not Data is being processed and if so, to obtain access to the Data and information mentioned by the GDPR, as well as to obtain a copy of your Personal Data.

- **Right to Request Rectification of Personal Data**: allows you to correct and supplement any incomplete or inaccurate Data we hold; however, we may need to verify the accuracy of new Data provided.

- **Right to request deletion of Personal Data ("right to be forgotten")**: allows you to request the removal and deletion of your Personal Data where there is no valid reason to continue processing it. You can obtain the deletion of your Personal Data in the cases provided for in Article 17 GDPR. However, please note that in certain circumstances we may not be able to comply with your request for deletion for specific legal reasons (e.g., where it is necessary to enable you to comply with a legal obligation or to establish, exercise or defend a right in court) that will be communicated to you at the time of your request.

- **Right to object to the processing of Personal Data**: under the terms of Article 21 GDPR, you may object to the processing of the Data, for reasons related to your particular situation, in cases where we, or a third party, should rely on legitimate interest and should you believe that such processing in any way infringes upon your fundamental rights and freedoms. In which case, the Company will refrain from further processing Personal Data unless the Company demonstrates the existence of compelling legitimate grounds for processing that override your interests, rights and freedoms or for the establishment, exercise or defense of a legal claim.

- **Right to request restriction of the 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 if an exception to this request is applicable (e.g. in the case where the processing is unlawful and you object to the deletion of the Data, requesting that its use be restricted).

- **Right to request the transfer of Personal Data to you or a third party ("data portability")**: we will deliver your Personal Data to you or to a party delegated by you in a structured, commonly used and machine-readable format, under the conditions set out in Article 20 GDPR. Please note that this right applies only to information processed by automated means and for processing that takes place on the basis of consent, or as part of the fulfillment of the contract entered into with you.

- **Right to Revoke Consent at Any Time**: Limited to any processing based on your consent (as collected from time to time by Scalapay IP following the provision of appropriate notice) you will have the right to revoke your consent given for consent-based processing of Personal Data at any time and we will cease to use your Personal Data, but without affecting the lawfulness of the processing based on the consent given prior to revocation.

- **Right to file a complaint with the authority**: we remind you that you always have the right to file a complaint with the Italian Data Protection Authority, based at Piazza Venezia 11, Rome, at the e-mail address: protocollo@gpdp.it.

10. COOKIE

Scalapay IP does not use any type of cookies. This means that while you are browsing our site (at the https://paymentinstitute.scalapay.com/ link), we do not collect any information on your device, such as browsing data or preferences. We do not use third-party cookies for tracking or personalized 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 can contact us by e-mail at scalapayip@legalmail.it and we will do what we can to help you.

In addition, if you have questions regarding the processing of personal data, including requests to exercise your rights, you can also contact our DPO using the following e-mail address: privacy@ip.scalapay.com.