

SCALAPAY IP S.p.A. – POLITIQUE DE CONFIDENTIALITÉ

Scalapay IP S.p.A., un établissement de paiement constitué conformément au droit italien, dont le siège social est situé Via Nervesa, 21, 20139 Milan (MI), numéro fiscal et numéro de TVA 06078740484, exerçant ses activités en vertu des articles 114-sexies et suivants du Décret législatif n. 385 du 1er septembre 1993 (le « **Texte Unique Bancaire** » ou « **TUB** »), inscrit sous le numéro 36018.0 au Registre des Établissements de Paiement visé à l'article 114-septies du TUB et soumis à la surveillance de la Banque d'Italie (ci-après également dénommée « **Scalapay IP** » ou « **Responsable du Traitement** » ou « **Responsable** » ou « **Société** »), agissant en qualité de responsable du traitement, respecte votre vie privée et s'engage à protéger vos données personnelles. Scalapay IP s'engage à traiter vos données conformément au Règlement Général sur la Protection des Données (Règlement UE 2016/679), communément désigné sous le terme « **RGPD** », ainsi qu'à toute autre loi applicable en matière de protection de la vie privée.

La présente politique de confidentialité expose les motifs, les modalités de collecte, de gestion et de protection des données personnelles relatives aux **clients des services de Scalapay IP, ci-après également désignés « Consommateurs » (SECTION A)**, ainsi qu'aux **vendeurs affiliés de Scalapay IP, ci-après également désignés « Merchant » (SECTION B)**.

En particulier, les traitements des données personnelles effectués par Scalapay IP seront conduits dans le respect des principes de licéité, de loyauté, de transparence, de limitation des finalités et de la conservation, de minimisation des données, d'exactitude, d'intégrité et de confidentialité.

Scalapay IP a désigné un Délégué à la Protection des Données (le « **Data Protection Officer** » ou « **DPO** »), qui peut être contacté par les personnes concernées pour obtenir des réponses relatives aux traitements des données personnelles effectués par le Responsable du Traitement, tant à l'égard des Consommateurs que des Merchant à l'adresse suivante: privacy@ip.scalapay.com.

Il est important que vous lisiez la présente politique de confidentialité, ainsi que toute autre politique de confidentialité que nous pourrions fournir pour compléter, mettre à jour ou approfondir les informations relatives à la collecte et au traitement de vos données personnelles. Nous nous efforcerons de coordonner ces politiques de confidentialité de manière à représenter à tout moment les conditions appliquées au traitement de vos données personnelles de la façon la plus transparente et la plus facilement accessible.

* * *

SECTION A – POLITIQUE DE CONFIDENTIALITÉ DES CONSOMMATEURS

1. RESPONSABLE DU TRAITEMENT

La présente politique de confidentialité est rédigée conformément aux articles 13 et 14 du RGPD et a pour objet de vous fournir les informations relatives à la manière dont Scalapay IP traite vos données personnelles en qualité de responsable du traitement. Vos données personnelles sont collectées par l'utilisation du site web www.scalapay.com et de l'application Scalapay (ci-après, la « **Plateforme Scalapay** ») lorsque vous décidez d'utiliser l'un des services offerts par Scalapay IP, grâce auxquels vous, en qualité de consommateur (ci-après également « **Consommateur** » ou « **Personne Concernée** »), pouvez acheter des produits et services auprès des vendeurs affiliés (ci-après, les « **Merchant** ») par le biais de l'un des services de paiement proposés par Scalapay IP (par exemple: Pay in 3; Pay in 4; Pay in 6, 9, 12; Pay Later; One Time Card ou Pay Now–Cart Saver via one time card ou BNPL traditionnel). Aux fins de l'exécution du contrat conclu avec le Merchant, Scalapay IP traite également des données personnelles collectées auprès des Merchant et/ou de Scalapay S.r.l.

2. DESCRIPTION DU TRAITEMENT

Afin de faciliter la compréhension des activités de traitement menées par Scalapay IP, nous présentons ci-après un tableau récapitulatif : (i) les catégories de données personnelles traitées, (ii) les finalités du traitement, (iii) la « base juridique » qui autorise chaque traitement et lui confère sa licéité, ainsi que (iv) la durée pendant laquelle Scalapay IP conservera vos données personnelles (les « **Données Personnelles** » ou « **Données** »).

Catégorie de Données Personnelles	Finalité du traitement	Base juridique	Durée de conservation
Données de contact et d'identification du Consommateur, informations relatives aux paiements. Par exemple, prénom, nom, numéro d'identification fiscale, adresse de résidence (pays, province, ville, code postal), adresse de livraison, lieu de naissance, date de naissance, genre, adresse e-mail, numéro de téléphone mobile, nationalité, document d'identité (type, numéro, date d'émission, autorité émettrice, ville). Informations relatives aux biens/services achetés ou commandés, tels que le type d'article et la catégorie du Merchant auprès duquel les achats sont effectués.	Fourniture des services de paiement aux Consommateurs (Pay in 3, Pay in 4, Pay Later ou carte de paiement virtuelle) et des activités suivantes : – Envoi d'e-mails relatifs à la transaction ; – Transmission des informations au Merchant pour l'exécution du contrat; – Assistance en cas de demande du Consommateur.	Exécution d'un contrat auquel le Consommateur est partie ou exécution de mesures précontractuelles prises à la demande du Consommateur (article 6, paragraphe 1, point b) du RGPD).	10 (dix) ans après la cessation du contrat.
Données biométriques du Consommateur (notamment, à partir des caractéristiques du visage du Consommateur extraites du selfie ou du vidéo-selfie réalisé par le Consommateur).	Effectuer la vérification préalable de la clientèle par identification biométrique du visage du Consommateur.	Obligation légale à laquelle le Responsable du Traitement est soumis et poursuite d'un intérêt public (article 6, paragraphe 1, points c) et e) du RGPD, ainsi qu'article 9, paragraphe 2, point g) du RGPD, en combinaison avec l'article 2-sexies du Décret législatif n° 196/2003) aux fins de la réglementation en matière de lutte contre le blanchiment de capitaux et de prévention des fraudes, comme expressément prévu par la réglementation sectorielle (Décret législatif n. 231/2007).	10 (dix) ans à compter de l'achèvement du processus de vérification préalable.
Données contenues dans le document d'identité du Consommateur et selfie ou vidéo-selfie réalisé par le Consommateur dans le cadre de la procédure de vérification de l'identité.		Obligation légale à laquelle le Responsable du traitement est soumis et poursuite d'un intérêt public (article 6, paragraphe 1, points c) et e) du RGPD), aux fins de la législation relative à la lutte contre le blanchiment de capitaux et de la prévention de la	

Catégorie de Données Personnelles	Finalité du traitement	Base juridique	Durée de conservation
		fraude, comme expressément prévu par la réglementation sectorielle applicable (décret législatif n° 231/2007).	
Image du visage de la Personne Concernée. Données contenues dans le document d'identité.	Effectuer la vérification préalable de la clientèle – par le biais de la Vérification Alternative (telle que définie et décrite à la Section 4) – en comparant l'image du visage du Consommateur avec l'image du visage figurant dans le document d'identité.	Obligation légale à laquelle le Responsable du traitement est soumis et poursuite d'un intérêt public (article 6, paragraphe 1, points c) et e) du RGPD), aux fins de la législation relative à la lutte contre le blanchiment de capitaux et à la prévention de la fraude, comme expressément prévu par la réglementation sectorielle applicable (décret législatif n° 231/2007).	10 (dix) ans à compter de l'achèvement du processus de vérification préalable.
Images et vidéos acquises auprès du Consommateur (selfie ou vidéo-selfie) et données contenues dans les documents d'identité.	Effectuer des contrôles supplémentaires de vérification de l'identité basés sur des technologies d'intelligence artificielle (« IA ») appliquées aux images et vidéos fournies par le Consommateur, afin de vérifier la correspondance avec les documents d'identité et de prévenir les fraudes ou utilisations abusives des services.	Obligation légale à laquelle le Responsable du traitement est soumis et poursuite d'une mission d'intérêt public (article 6, paragraphe 1, points c) et e) du RGPD), conjointement avec le décret législatif n° 196/2003, et aux fins de la législation relative à la lutte contre le blanchiment de capitaux (décret législatif n° 231/2007) et à la prévention de la fraude.	10 (dix) ans à compter de l'achèvement du processus de vigilance à l'égard de la clientèle ou, en tout cas, jusqu'à l'achèvement des vérifications effectuées au moyen de l'IA.
Données d'identification figurant sur le document d'identité (par exemple: prénom, nom, date et lieu de naissance, date de délivrance et date d'expiration du document), y compris les données collectées au moyen d'outils automatisés lorsque la procédure de vigilance à l'égard de la clientèle par identification biométrique ne peut être menée.	Lorsque le processus d'identification biométrique ne permet pas de capturer correctement certaines informations contenues dans le document d'identité (telles que la date de délivrance et la date d'expiration), ces données peuvent être acquises au moyen d'un système automatisé de lecture (OCR – reconnaissance optique de caractères).	Obligation légale à laquelle le Responsable du traitement est soumis et poursuite d'un intérêt public (article 6, paragraphe 1, points c) et e) du RGPD) aux fins de la législation relative à la lutte contre le blanchiment de capitaux et à la prévention de la fraude, comme expressément prévu par la réglementation sectorielle applicable (décret législatif n° 231/2007).	La donnée est supprimée à l'issue du processus de lecture.

Catégorie de Données Personnelles	Finalité du traitement	Base juridique	Durée de conservation
Données d'identification figurant sur le document d'identité (par exemple: prénom, nom, date et lieu de naissance, date de délivrance et date d'expiration du document, image du visage).	Vérification documentaire effectuée dans le cadre du processus de vigilance à l'égard de la clientèle au moyen d'un système basé sur l'intelligence artificielle. Analyse automatisée de l'image du document (avant la capture du selfie) afin d'en vérifier l'authenticité, l'intégrité et la présence éventuelle de signes de falsification ou d'altération, à la suite de son téléchargement par le Consommateur.	Obligation légale à laquelle le Responsable du traitement est soumis et poursuite d'un intérêt public (article 6, paragraphe 1, points c) et e) du RGPD) aux fins de la législation relative à la lutte contre le blanchiment de capitaux et à la prévention de la fraude, comme expressément prévu par la réglementation sectorielle applicable (décret législatif n° 231/2007).	10 (dix) ans à compter de l'achèvement du processus de vigilance à l'égard de la clientèle.
Données financières et relatives aux paiements (par exemple, quatre derniers chiffres de la carte, date d'expiration et lieu d'émission, IBAN).	Traitement du paiement de la commande et gestion des encaissements et des paiements.	Exécution d'un contrat auquel le Consommateur est partie ou mise en œuvre de mesures précontractuelles prises à la demande du Consommateur (article 6, paragraphe 1, point b) du RGPD).	10 (dix) ans après la cessation du contrat.
	Gestion de l'Archive Unique Informatique (AUI), notamment les déclarations effectuées pour satisfaire aux obligations réglementaires et de déclaration à l'égard de la Banque d'Italie.	Obligation légale à laquelle le Responsable du Traitement est soumis (article 6, paragraphe 1, point c) du RGPD).	10 (dix) ans à compter de l'enregistrement de la déclaration.
Données fournies spontanément par le Consommateur.	Répondre aux demandes du Consommateur (par exemple, en cas de demande d'assistance pour effectuer la vérification préalable).	Exécution d'un contrat auquel le Consommateur est partie ou mise en œuvre de mesures précontractuelles prises à la demande du Consommateur (article 6, paragraphe 1, point b) du RGPD).	Pour le temps nécessaire à répondre au Consommateur et, en tout cas, pour une durée ne pas excédant 2 (deux) ans.
Toutes les Données Personnelles indiquées dans le présent tableau (à l'exception des données biométriques).	Gestion des éventuels litiges avec les Consommateurs.	Poursuite de l'intérêt légitime du Responsable du Traitement aux fins de la constatation, de l'exercice ou de la défense d'un droit en justice, ou chaque fois que les autorités judiciaires exercent leurs fonctions juridictionnelles (article 6, paragraphe 1, point f) du RGPD).	Jusqu'à la conclusion du litige.

Catégorie de Données Personnelles	Finalité du traitement	Base juridique	Durée de conservation
Données d'identification (prénom, nom, numéro d'identification fiscale, date et lieu de naissance), coordonnées, données relatives aux transactions, données relatives à la demande d'utilisation des services de paiement en plusieurs fois, ainsi que données relatives au comportement de paiement (y compris toute information relative à des retards de paiement ou à des défauts de paiement).	Évaluation de la solvabilité et du risque de crédit du Consommateur demandant l'utilisation de l'un des instruments de paiement proposés par le Responsable du traitement, prévention du risque de fraude, prévention du surendettement et gestion responsable du risque de crédit. À ces fins, Scalapay IP peut : - consulter des systèmes d'information sur le crédit (« SIC »), tels que CRIF S.p.A. ; - communiquer à ces mêmes SIC des informations relatives à la demande d'utilisation des services, à l'issue de cette demande et au comportement de paiement.	Exécution d'un contrat auquel le Consommateur est partie ou mise en œuvre de mesures précontractuelles prises à la demande du Consommateur (article 6, paragraphe 1, point b) du RGPD), ainsi que la poursuite de l'intérêt légitime du Responsable du traitement à assurer une gestion appropriée du risque de crédit, la prévention de la fraude et le respect des principes de gestion saine et prudente (article 6, paragraphe 1, point f) du RGPD). Le traitement a fait l'objet d'un test de mise en balance conformément au RGPD.	Traitement par les SIC Les données communiquées aux SIC seront traitées et conservées par ces entités conformément aux modalités prévues par le Code de conduite applicable aux systèmes d'information sur le crédit et par la législation applicable.
Données relatives à la situation professionnelle et financière du Consommateur, collectées dans le cadre d'une demande d'utilisation du service Pay in 6, 9, 12. En particulier : type d'occupation, type de contrat de travail, secteur d'emploi (public/privé), revenu net mensuel, nom de l'employeur, accomplissement de la période d'essai, existence et montant mensuel des obligations financières fixes (loyer ou emprunt immobilier), existence et montant des autres prêts ou financements en cours.	Évaluation interne de la solvabilité et du risque de crédit du Consommateur demandant l'utilisation du service Pay in 6, 9, 12, afin de déterminer si la transaction peut être approuvée, préalablement à toute consultation des systèmes d'information sur le crédit (SIC).	Exécution d'un contrat auquel le Consommateur est partie ou mise en œuvre de mesures précontractuelles prises à la demande du Consommateur (article 6, paragraphe 1, point b) du RGPD).	10 (dix) ans après la cessation du contrat.

Catégorie de Données Personnelles	Finalité du traitement	Base juridique	Durée de conservation
Données d'identification sous forme pseudonymisée. Données relatives aux transactions déjà effectuées en utilisant les services du Responsable (montant des transactions, dates des transactions et des échéances des versements, statut des paiements).	Analyse de l'intégration entre la technologie de Scalapay IP et des composants tiers afin d'atteindre les objectifs suivants : - évaluation précise de la solvabilité et du risque de crédit des Consommateurs demandant l'utilisation de l'un des instruments de paiement proposés par le Responsable du traitement; - évaluation appropriée de la fiabilité et de la ponctualité des paiements des Consommateurs; - prévention du risque de fraude, y compris la prévention du vol d'identité.	Poursuite de l'intérêt légitime du Responsable du traitement (article 6, paragraphe 1, point f) du RGPD). Ce traitement est nécessaire pour permettre à Scalapay IP d'assurer une gestion responsable des risques, de prévenir la fraude et de protéger les consommateurs contre le surendettement. Le traitement a fait l'objet d'un test de mise en balance afin de garantir qu'il ne porte pas atteinte aux droits et libertés fondamentaux du Consommateur.	60 (soixante) jours à compter de l'analyse du risque.

3. LIENS VERS DES SITES TIERS

La Plateforme Scalapay, à laquelle vous accédez pour effectuer des achats en plusieurs fois auprès des Merchant, peut inclure des liens vers des sites web de tiers (par exemple, les sites web des boutiques auprès desquelles vous achetez des produits ou services). En cliquant sur ces liens ou en les activant, il est possible que des tiers traitent vos Données Personnelles ; par conséquent, nous vous invitons à consulter également la politique de confidentialité de ces sites, ainsi que la politique de confidentialité de la Plateforme Scalapay.

4. SI VOUS NE FOURNISSEZ PAS VOS DONNÉES PERSONNELLES

Dans certains cas, nous devons collecter vos Données Personnelles pour satisfaire à une obligation légale ou en vertu des termes d'un contrat que nous avons avec vous ou que nous cherchons à conclure avec vous (par exemple, pour autoriser le paiement différé). Dans ces cas, le défaut de fourniture des Données Personnelles empêchera Scalapay IP de conclure un contrat avec vous.

En particulier, afin de respecter la réglementation sectorielle applicable à la Société, la fourniture des Données à des fins de vérification biométrique est obligatoire pour nous permettre d'effectuer la vérification de l'identité en ligne. En tout état de cause, lorsque le Consommateur ne peut pas, en raison de limitations techniques de son appareil, procéder à la vérification de son identité en ligne, ou lorsqu'il a épuisé les tentatives de vérification de l'identité mises à sa disposition par la Société, le Consommateur peut envoyer un e-mail à l'adresse support@scalapay.com en joignant (i) une photographie d'un document d'identité en cours de validité (ou d'un document équivalent) et (ii) une photographie sur laquelle le visage du Consommateur et le document d'identité tenu en main sont visibles. Le personnel de la Société procédera manuellement à la vérification de l'identité (« **Vérification Alternative** »). Dans ce cas, aucune donnée biométrique du Consommateur ne sera traitée.

En ce qui concerne spécifiquement le service Pay in 6, 9, 12, la fourniture des données relatives à la situation professionnelle et financière (telles que, à titre d'exemple, le type d'occupation, le revenu net mensuel, l'existence d'obligations financières fixes et d'autres financements en cours) est obligatoire aux fins de l'évaluation de la solvabilité requise par la réglementation applicable. Le défaut de fourniture de ces données empêchera Scalapay IP de procéder à l'évaluation de la demande et, par conséquent, de fournir le service Pay in 6, 9, 12.

5. TRANSFERTS INTERNATIONAUX

Certains de nos prestataires sont établis en dehors de l'Union européenne. Lorsque nous transférons vos Données à ces prestataires, nous nous assurons que vos Données sont traitées et protégées d'une manière substantiellement équivalente au niveau de protection applicable au sein de l'UE. À cet égard, dans le respect des garanties prévues par le RGPD, vos données sont transférées sur la base de :

- Décisions d'adéquation : lorsque le transfert de données personnelles s'effectue vers des pays que la Commission européenne a reconnus comme offrant un niveau de protection adéquat des données personnelles;
- Clauses contractuelles types : en l'absence de décisions d'adéquation, nous aurons recours à des contrats spécifiques approuvés par la Commission européenne, visant à garantir le même niveau de protection des données personnelles que celui prévu au sein du territoire européen.

La liste des pays situés en dehors de l'Union européenne vers lesquels Scalapay IP peut transférer vos données (y compris les informations sur les garanties adoptées) est disponible sur demande, en nous contactant aux coordonnées indiquées dans la présente politique de confidentialité.

6. À QUI POUVONS-NOUS COMMUNIQUER VOS DONNÉES PERSONNELLES ?

Au sein de l'organisation de Scalapay IP, les Données pourront être traitées par les agents des services compétents pour l'exécution des différentes activités de traitement.

En outre, afin de fournir nos services, nous pourrions communiquer vos Données Personnelles aux catégories de destinataires énumérés ci-dessous, pour les finalités indiquées, dans le respect des principes de minimisation et de limitation des finalités, et en mettant en œuvre les mesures de sécurité appropriées. L'identification précise des destinataires auxquels nous communiquerons vos Données Personnelles dépendra des services que vous utiliserez. En particulier, pour la fourniture des services, les catégories de parties auxquelles nous communiquerons les Données, dans le cadre et dans la limite des finalités poursuivies, sont les suivantes :

- Prestataires : nous pourrions communiquer des Données Personnelles à des prestataires – avec lesquels nous concluons des accords contractuels – que nous utilisons pour vous fournir des services. Parmi ces prestataires figurent, à titre d'exemple, des fournisseurs de logiciels et de stockage de données, des services de traitement des paiements, des conseillers en affaires, des sociétés fournissant des logiciels de scan biométrique du visage des Consommateurs et des sociétés de réseau d'affiliation.
- Augusta SPV S.r.l. : Scalapay IP pourra communiquer vos Données Personnelles à la société Augusta SPV S.r.l., véhicule de titrisation de créances en vertu de la loi n° 130 du 30 avril 1999, en tant qu'entité impliquée dans l'opération de titrisation pour la fourniture aux Consommateurs des instruments de paiement.
- Scalapay S.r.l. : Scalapay IP pourrait communiquer vos Données Personnelles à la société Scalapay S.r.l. en tant qu'opérateur de la Plateforme Scalapay sur laquelle vous avez créé un profil utilisateur.
- Boutiques en ligne et physiques : Scalapay IP peut communiquer des Données Personnelles à la boutique en ligne auprès de laquelle vous effectuez un achat. Ceci est fait dans le but de permettre à la boutique d'administrer votre achat et votre relation avec la boutique, de vous expédier les marchandises, de gérer d'éventuels litiges et de prévenir les fraudes. Les données personnelles communiquées à une boutique seront soumises à ce qui est indiqué dans la politique de confidentialité de la boutique elle-même.
- Prestataires de services de paiement (« PSP ») : les PSP permettent d'accepter des paiements électroniques par le biais d'un large éventail de méthodes de paiement, telles que les cartes de crédit, les paiements bancaires comme le prélèvement automatique, etc.
- Sociétés de recouvrement de créances : Scalapay IP pourrait avoir la nécessité de partager vos Données lors de la cession ou de l'externalisation du recouvrement de créances échues et impayées à des tiers, tels qu'une société de recouvrement de créances.

- Systèmes d'Information sur le Crédit (SIC) : Scalapay IP peut communiquer les Données Personnelles du Consommateur à des SIC, tels que CRIF S.p.A., aux fins d'évaluation de la solvabilité, de prévention des fraudes et de gestion du risque de crédit. Ces entités agissent en qualité de responsables autonomes du traitement.
- Autorités : Scalapay IP pourrait fournir des informations jugées nécessaires aux autorités de police, financières, fiscales ou autres autorités et tribunaux, y compris la Banque d'Italie ou l'Agence des Revenus. Les Données Personnelles sont partagées avec l'autorité lorsque cela est prévu par la loi, dans certains cas à votre demande, ou lorsque cela est nécessaire pour la gestion des déductions fiscales, la lutte contre la criminalité ou la protection de nos droits en justice ou en dehors de toute procédure judiciaire. Un exemple d'obligation légale de fournir des informations se présente lorsqu'il est nécessaire de prendre des mesures contre le blanchiment d'argent et le financement du terrorisme.

Ces entités auront accès aux Données Personnelles nécessaires à l'exercice des fonctions régies par un accord entre les sociétés, et agiront – selon les cas – en qualité de responsables autonomes du traitement ou de sous-traitants (dans ce dernier cas, en vertu d'un accord de désignation en qualité de sous-traitant conformément à l'article 28 du RGPD).

7. UTILISATION DES SYSTÈMES D'INFORMATION SUR LE CRÉDIT (SIC)

Lorsque le Consommateur demande à utiliser l'un des services de paiement fractionné offerts par Scalapay IP, à l'exclusion du service Pay in 6, 9, 12, le Responsable pourra consulter un ou plusieurs SIC, tels que, à titre d'exemple, CRIF S.p.A., aux fins d'évaluation de la solvabilité et de la fiabilité du Consommateur.

Dans le cadre de cette activité :

- Scalapay IP pourra communiquer aux SIC les données d'identification du Consommateur. Les données relatives à la situation professionnelle et financière collectées dans le cadre du service Pay in 6, 9, 12 sont traitées exclusivement par Scalapay IP aux fins de l'évaluation interne de la solvabilité et ne sont pas communiquées aux SIC ni à d'autres tiers
- les SIC pourront fournir à Scalapay IP des informations sur le profil de crédit du Consommateur.

Cet échange d'informations vise à :

- évaluer la fiabilité et la ponctualité des paiements ;
- prévenir les situations de surendettement ;
- prévenir et combattre les fraudes ou les utilisations indues des services ;
- garantir une gestion responsable et prudente du risque de crédit.

Les Systèmes d'Information sur le Crédit agissent en qualité de responsables autonomes du traitement et traitent les données dans le respect du Code de Conduite pour les Systèmes d'Information sur le Crédit et de la réglementation applicable.

Pour de plus amples informations sur les modalités de traitement des données par les SIC et sur les durées de conservation correspondantes, le Consommateur peut consulter la politique de confidentialité mise à disposition par ces entités (par exemple, pour CRIF S.p.A., sur leur [site institutionnel](#)).

8. PENDANT COMBIEN DE TEMPS UTILISERONS-NOUS VOS DONNÉES ?

De plus amples informations sur la durée de conservation figurent dans le tableau de la Section 2. Nous conservons vos Données uniquement pour la durée nécessaire à la réalisation des finalités pour lesquelles elles ont été collectées, telles que l'exécution du contrat ou le respect des obligations légales. Lorsque nous décidons de la durée de conservation de vos Données, nous prenons en considération la quantité et le type de Données, leur sensibilité et le risque d'utilisation abusive.

À l'expiration de la durée de conservation, les Données Personnelles seront supprimées ou anonymisées. Par conséquent, à l'expiration de ce délai, la personne concernée pourrait ne plus être en mesure d'exercer les droits visés à la Section 9 (tels que le droit d'accès, d'effacement, de rectification et le droit à la portabilité des Données Personnelles).

9. TRAITEMENT DE VÉRIFICATION BIOMÉTRIQUE. ABSENCE DE PRISE DE DÉCISION AUTOMATISÉE

La Société utilise des technologies biométriques pour effectuer la vérification de l'identité des Consommateurs qui souhaitent utiliser les services de paiement offerts par Scalapay IP. Comme indiqué à la Section 2, ce traitement est effectué afin de satisfaire aux obligations légales en matière de prévention du blanchiment d'argent et du financement du terrorisme, telles que requises par la réglementation en matière de lutte contre le blanchiment d'argent (y compris le Décret législatif n° 231/2007).

En dehors du cas de la Vérification Alternative (qui, comme indiqué à la Section 4, ne s'applique qu'à titre résiduel), le processus de vérification de l'identité est effectué par des technologies de vérification faciale reposant sur une comparaison individuelle (entre l'image de votre visage capturée par le selfie ou la vidéo et celle figurant dans le document d'identité que vous fournirez). Pour effectuer cette vérification, nous vous demanderons de :

- télécharger une photographie de votre document d'identité (ou d'un document équivalent) directement sur la Plateforme Scalapay ;
- prendre un selfie ou enregistrer une courte vidéo à l'aide de l'appareil photo de votre dispositif, en suivant des instructions spécifiques garantissant la bonne acquisition de l'image (par exemple, des conditions d'éclairage adéquates et l'absence d'autres personnes dans le champ).

Nous procéderons à un contrôle de vos données biométriques (le selfie ou la vidéo mentionnés précédemment) pour vérifier la correspondance de votre visage avec la photographie figurant dans le document d'identité concerné, en vérifiant la cohérence des informations contenues dans le document d'identité avec celles que vous avez fournies, ainsi que le cadrage et les conditions environnementales. Vous serez en tout état de cause toujours informé de la collecte de la donnée biométrique. De plus, Scalapay IP ne prendra jamais – par le biais du processus décrit ci-dessus – de décisions fondées uniquement sur des traitements automatisés produisant des effets juridiques ou vous affectant de manière analogue et significative. En effet, si la vérification n'aboutit pas, le personnel de la Société sera toujours impliqué pour en évaluer les raisons.

Pour de plus amples informations sur le type de technologie utilisée par la Société et, en tout état de cause, pour exercer ces droits, il est possible de contacter notre délégué à la protection des données (DPO) aux adresses indiquées ci-dessous.

En cas d'utilisation d'outils automatisés pour l'extraction de données à partir de documents d'identité, ces systèmes ne déterminent pas de manière autonome l'issue du processus de vérification, mais soutiennent exclusivement l'activité d'identification, qui est complétée par du personnel autorisé ou par des contrôles supplémentaires.

Les vérifications de l'identité prévoient également un contrôle de la fiabilité de l'image du document fourni, tant par une comparaison entre les vidéos et les images du visage acquises lors du processus d'identification et les images figurant dans le document, que par l'analyse des éléments qui rendent un document d'identité fiable. Ces contrôles sont effectués par un système d'IA, qui n'acquiert pas de données supplémentaires et ne mémorise pas les informations figurant sur les documents. Outre le respect des obligations réglementaires relatives à la correcte identification de la personne concernée, les contrôles ont pour objectif de prévenir d'éventuelles fraudes, pour une meilleure protection des services et des clients eux-mêmes. Les technologies d'IA utilisées opèrent dans le respect des principes de licéité, de loyauté, de transparence, de proportionnalité et de minimisation des données, et ne conduisent pas à des décisions fondées uniquement sur des traitements automatisés produisant des effets juridiques ou affectant significativement la personne concernée.

9bis. ABSENCE DE PRISE DE DÉCISION AUTOMATISÉE POUR L'ÉVALUATION DE LA SOLVABILITÉ

Dans le cadre de l'évaluation de la solvabilité, et en particulier pour le service Pay in 6, 9, 12, Scalapay IP peut utiliser des outils d'analyse automatisée tenant compte également des informations provenant des SIC, ainsi que des données relatives à la situation professionnelle et financière du Consommateur (telles que le type d'occupation, le revenu net mensuel, les obligations financières fixes et les autres financements en cours) fournies par le Consommateur. En tout état de cause, ces outils n'entraînent pas l'adoption de décisions fondées uniquement sur des traitements automatisés produisant des effets juridiques ou affectant de manière analogue et significative la Personne Concernée, une intervention humaine adéquate étant toujours prévue dans les cas où cela s'avère nécessaire.

10. VOS DROITS

Nous vous rappelons que vous pouvez exercer vos droits relatifs aux données personnelles selon les modalités et dans les limites prévues par les lois sur la protection des données. Vous trouverez ci-après une brève description de ces droits que vous pourrez exercer lorsque les conditions prévues par le RGPD seront réunies :

- **Droit d'être informé** : toutes les personnes physiques ont le droit d'être informées sur la collecte et l'utilisation de leurs Données Personnelles. Il s'agit d'une exigence fondamentale de transparence telle qu'établie par le RGPD. La présente Politique de Confidentialité et les réponses que nous fournirons à vos demandes satisfont à cette exigence.
- **Droit de demander l'accès aux Données Personnelles** : connu sous le nom de « demande d'accès », il permet d'obtenir la confirmation que des Données font ou ne font pas l'objet d'un traitement et, dans l'affirmative, d'obtenir l'accès aux Données et aux informations mentionnées par le RGPD, ainsi qu'une copie de vos Données Personnelles.
- **Droit de demander la rectification des données personnelles** : il vous permet de corriger et de compléter les éventuelles Données incomplètes ou inexacts en notre possession ; cependant, nous pourrions avoir besoin de vérifier l'exactitude des nouvelles données fournies.
- **Droit de demander l'effacement des données personnelles (« droit à l'oubli »)** : il vous permet de demander la suppression et l'effacement de vos Données Personnelles lorsqu'il n'existe pas de motifs valables pour continuer à les traiter. Vous pouvez obtenir l'effacement de vos Données Personnelles dans les cas prévus à l'article 17 du RGPD. Toutefois, nous vous informons que dans certains cas, nous pourrions ne pas être en mesure de satisfaire votre demande d'effacement pour des raisons légales spécifiques (par exemple, lorsque cela est nécessaire pour vous permettre de remplir une obligation légale ou pour constater, exercer ou défendre un droit en justice) qui vous seront communiquées au moment de votre demande.
- **Droit de s'opposer au traitement des données personnelles** : dans les termes prévus à l'article 21 du RGPD, vous pouvez vous opposer au traitement des Données, pour des motifs tenant à votre situation particulière, dans les cas où nous, ou un tiers, nous fondons sur l'intérêt légitime et où vous estimez que ce traitement porte atteinte d'une quelconque manière à vos droits et libertés fondamentaux. Dans ce cas, la Société s'abstiendra de traiter davantage les Données Personnelles, sauf si la Société démontre l'existence de motifs légitimes impérieux pour le traitement qui prévalent sur vos intérêts, droits et libertés, ou pour la constatation, l'exercice ou la défense d'un droit en justice. Pour exercer ce droit, vous pouvez nous contacter à l'adresse privacy@ip.scalapay.com.
- **Droit de demander la limitation du traitement des données personnelles** : vous pouvez demander la limitation du traitement de vos Données Personnelles dans les cas prévus à l'article 18 du RGPD (par exemple, lorsque le traitement est illicite et que vous vous opposez à l'effacement des Données, en demandant que leur utilisation soit limitée).
- **Droit de demander le transfert des données personnelles vers vous ou vers un tiers (« portabilité des données »)** : nous vous remettons, ou à un tiers que vous aurez désigné, vos Données Personnelles dans un format structuré, couramment utilisé et lisible par machine, dans les conditions prévues à l'article 20 du RGPD. Nous vous rappelons que ce droit s'applique uniquement aux informations traitées par des moyens automatisés et aux traitements effectués sur la base du consentement, ou dans le cadre de l'exécution d'un contrat conclu avec vous.
- **Droit de retirer le consentement à tout moment** : en ce qui concerne les éventuels traitements basés sur votre consentement (tel que recueilli de temps à autre par Scalapay IP après la fourniture d'une politique de confidentialité appropriée), vous aurez le droit de retirer à tout moment le consentement donné pour les traitements de Données Personnelles basés sur le consentement, et nous cesserons d'utiliser vos Données Personnelles, sans toutefois affecter la licéité du traitement basé sur le consentement donné avant son retrait.

- **Droit d'introduire une réclamation auprès de l'autorité** : nous vous rappelons que vous avez toujours le droit d'introduire une réclamation auprès de l'Autorité Garante pour la Protection des Données Personnelles, dont le siège est situé Piazza Venezia 11, Rome, à l'adresse e-mail : protocollo@gpdp.it.

11. COOKIES

Scalapay IP n'utilise aucun type de cookie sur son site institutionnel (<https://paymentinstitute.scalapay.com/>). Cela signifie que lors de votre navigation sur notre site, nous ne collectons pas d'informations sur votre dispositif, telles que des données de navigation ou des préférences. Nous n'utilisons pas de cookies tiers à des fins de suivi ou de publicité personnalisée et nous ne partageons pas vos informations avec des tiers par le biais de cookies.

12. CONTACTS

Pour exercer vos droits ou pour demander des informations sur la manière dont nous traitons vos Données Personnelles, vous pouvez nous contacter par e-mail à l'adresse scalapayip@legalmail.it et nous ferons tout notre possible pour vous aider.

En outre, si vous avez des questions relatives au traitement des Données Personnelles, y compris des demandes d'exercice de vos droits, vous pouvez également contacter notre DPO à l'adresse e-mail suivante : privacy@ip.scalapay.com

* * *

SECTION B – POLITIQUE DE CONFIDENTIALITÉ DES MERCHANT

1. RESPONSABLE DU TRAITEMENT

La présente politique de confidentialité est rédigée conformément aux articles 13 et 14 du RGPD et a pour objet de vous fournir les informations relatives à la manière dont Scalapay IP traite vos données personnelles. Vos données personnelles ont été collectées par Scalapay S.r.l. par l'utilisation du site web www.scalapay.com et de la plateforme business (ci-après, la « **Plateforme Scalapay Business** ») ou par Scalapay IP lorsque vous concluez un contrat avec Scalapay IP en qualité de vendeur affilié (ci-après également « **Merchant** ») afin d'offrir à vos clients l'un des services de paiement proposés par Scalapay IP (par exemple: *Pay in 3; Pay in 4; Pay in 6, 9, 12; Pay Later; One Time Card* ou *Pay Now–Cart Saver* via one time card ou BNPL traditionnel).

2. DESCRIPTION DU TRAITEMENT

Afin de faciliter la compréhension des activités de traitement menées par Scalapay IP, nous présentons ci-après un tableau récapitulatif : (i) les catégories de données personnelles traitées, (ii) les finalités du traitement, (iii) la « base juridique » qui autorise chaque traitement et lui confère sa licéité, ainsi que (iv) la durée pendant laquelle Scalapay IP conservera vos données personnelles (« **Données Personnelles** » ou « **Données** »).

Catégorie de Données Personnelles	Finalité du traitement	Base juridique	Durée de conservation
Données de contact et d'identification du Merchant (par exemple : prénom, nom, adresse e-mail professionnelle et numéro de téléphone des employés du Merchant).	- Exécution du contrat conclu avec le Merchant ; - Création et gestion du profil du Merchant sur la plateforme Scalapay Business.	Exécution d'un contrat auquel la personne concernée est partie ou mise en œuvre de mesures précontractuelles prises à la demande de la personne concernée (article 6, paragraphe 1, point b) du RGPD).	10 (dix) ans à compter de la résiliation de la relation contractuelle.
Données biométriques du représentant autorisé ou du représentant légal du Merchant (notamment dérivées des caractéristiques faciales capturées à partir du selfie réalisé par le représentant autorisé ou le représentant légal).	Réalisation de la vigilance à l'égard de la clientèle.	Obligation légale à laquelle le Responsable du traitement est soumis et poursuite d'un intérêt public (article 6, paragraphe 1, points c) et e) du RGPD), ainsi que l'article 9, paragraphe 2, point g) du RGPD, conjointement avec l'article 2-sexies du décret législatif n° 196/2003 aux fins de la législation relative à la lutte contre le blanchiment de capitaux et à la prévention de la fraude, comme expressément prévu par la réglementation sectorielle applicable (décret législatif n° 231/2007).	10 (dix) ans à compter de l'achèvement du processus de vigilance à l'égard de la clientèle.
Données contenues dans le document d'identité du représentant autorisé ou du représentant légal du Merchant, ainsi qu'un selfie ou un selfie vidéo réalisé dans le cadre du processus de vérification.		Obligation légale à laquelle le Responsable du traitement est soumis et poursuite d'un intérêt public (article 6, paragraphe 1, points c) et	

		e) du RGPD) aux fins de la législation relative à la lutte contre le blanchiment de capitaux et à la prévention de la fraude, comme expressément prévu par la réglementation sectorielle applicable (décret législatif n° 231/2007).	
- Image du visage du représentant autorisé ou du représentant légal du Merchant ; - Données contenues dans le document d'identité.	Réalisation de la vigilance à l'égard de la clientèle -au moyen de la Vérification Alternative (telle que définie et décrite à la Section 4), -par comparaison entre l'image faciale du représentant autorisé ou légal et celle figurant sur le document d'identité.	Obligation légale à laquelle le Responsable du traitement est soumis et poursuite d'un intérêt public (article 6, paragraphe 1, points c) et e) du RGPD) aux fins de la législation relative à la lutte contre le blanchiment de capitaux et à la prévention de la fraude, comme expressément prévu par la réglementation sectorielle applicable (décret législatif n° 231/2007).	10 (dix) ans à compter de l'achèvement du processus de vigilance à l'égard de la clientèle.
Images et vidéos (selfie ou vidéo-selfie) du représentant autorisé ou du représentant légal du Merchant, ainsi que les données contenues dans les documents d'identité.	Réalisation de contrôles supplémentaires de vérification d'identité basés sur des technologies d'intelligence artificielle (« IA ») appliquées aux images et vidéos fournies afin de renforcer la vérification de correspondance.	Obligation légale à laquelle le Responsable du traitement est soumis et poursuite d'un intérêt public (article 6, paragraphe 1, points c) et e) du RGPD), conjointement avec le décret législatif n° 196/2003 et le décret législatif n° 231/2007 (législation relative à la lutte contre le blanchiment de capitaux et à la prévention de la fraude).	10 (dix) ans à compter de l'achèvement du processus de vigilance à l'égard de la clientèle ou, en tout état de cause, jusqu'à l'achèvement des vérifications effectuées au moyen de l'IA.
Données d'identification figurant dans le document d'identité (par exemple : prénom, nom, date et lieu de naissance, date de délivrance et date d'expiration du document), y compris les données collectées au moyen d'outils automatisés lorsque la procédure de vigilance par identification biométrique ne peut être menée à bien.	Lorsque le processus d'identification biométrique ne permet pas de capturer correctement certaines informations contenues dans le document d'identité (telles que les dates de délivrance et d'expiration), ces données peuvent être acquises au moyen d'un système automatisé de lecture (OCR – reconnaissance optique de caractères).	Obligation légale à laquelle le Responsable du traitement est soumis et poursuite d'un intérêt public (article 6, paragraphe 1, points c) et e) du RGPD) aux fins de la législation relative à la lutte contre le blanchiment de capitaux et à la prévention de la fraude, comme expressément prévu par la réglementation sectorielle applicable (décret législatif n° 231/2007).	Les données sont supprimées à l'issue du processus de lecture.
Données d'identification figurant dans le document d'identité (par exemple : prénom, nom, date et lieu de naissance, date de délivrance	Vérification documentaire effectuée dans le cadre du processus de vigilance à	Obligation légale à laquelle le Responsable du traitement est soumis et poursuite d'un intérêt	10 (dix) ans à compter de l'achèvement du processus de

et d'expiration du document, image du visage).	l'égard de la clientèle au moyen d'un système basé sur l'IA. Analyse automatisée de l'image du document (avant la capture du selfie) afin d'en vérifier l'authenticité, l'intégrité et la présence éventuelle de signes de falsification ou d'altération, après téléchargement par le Merchant.	public (article 6, paragraphe 1, points c) et e) du RGPD) aux fins de la législation relative à la lutte contre le blanchiment de capitaux et à la prévention de la fraude, comme expressément prévu par la réglementation sectorielle applicable (décret législatif n° 231/2007).	vigilance à l'égard de la clientèle.
Données personnelles relatives aux employés et/ou collaborateurs du Merchant fournies spontanément.	Fourniture d'une assistance au Merchant.	Exécution d'un contrat auquel la personne concernée est partie ou mise en œuvre de mesures précontractuelles prises à la demande de la personne concernée (article 6, paragraphe 1, point b) du RGPD).	Pendant le temps nécessaire pour répondre à la personne concernée et, en tout état de cause, pour une durée n'excédant pas 2 (deux) ans.
Données d'identification et données personnelles du Merchant en tant que personne physique (numéro d'identification fiscale et numéro de TVA).	Respect des obligations légales relatives à la transmission électronique des données à l'Agence fiscale italienne.	Respect d'une obligation légale à laquelle le Responsable du traitement est soumis et exécution d'une mission d'intérêt public conformément à l'article 6, paragraphe 1, points c) et e) du RGPD, conjointement avec l'article 22, paragraphes 5 et 6, du décret-loi n° 124/2019, converti en loi n° 157/2019, ainsi qu'avec la décision de mise en œuvre de l'Agence des recettes italienne et le protocole de mise en œuvre n° 142285/2025.	10 (dix) ans à compter de la date de l'addebit.

3. LIENS VERS DES SITES TIERS

La Plateforme Scalapay Business n'inclut pas de liens vers des sites web de tiers.

4. SI VOUS NE FOURNISSEZ PAS VOS DONNÉES PERSONNELLES

Dans certains cas, nous devons collecter vos Données Personnelles pour satisfaire à une obligation légale ou en vertu des termes d'un contrat que nous avons avec vous ou que nous cherchons à conclure avec vous. Dans ces cas, le défaut de fourniture des Données Personnelles empêchera Scalapay IP de conclure un contrat avec vous et/ou de vous fournir le service.

En particulier, afin de respecter la réglementation sectorielle applicable à la Société, la fourniture des Données à des fins de vérification biométrique est obligatoire pour nous permettre d'effectuer la vérification de l'identité en ligne. En tout état de cause, lorsque le représentant légal ou l'exécutant du Merchant ne peut pas, en raison de limitations techniques de son appareil, procéder à la vérification de son identité en ligne, ou lorsqu'il a épuisé les tentatives de vérification de l'identité offertes par la Société, le représentant légal ou l'exécutant du Merchant peut envoyer un e-mail à l'adresse support@scalapay.com en joignant (i) une photographie d'un document d'identité en cours de validité (ou d'un

document équivalent) et (ii) une photographie sur laquelle le visage du représentant légal ou de l'exécutant du Merchant et le document d'identité tenu en main sont visibles. Le personnel de la Société procédera manuellement à la vérification de l'identité (« **Vérification Alternative** »). Dans ce cas, aucune donnée biométrique du représentant légal ou de l'exécutant du Merchant ne sera traitée.

5. TRANSFERTS INTERNATIONAUX

Certains de nos prestataires sont établis en dehors de l'Union européenne. Lorsque nous transférons vos Données à ces prestataires, nous nous assurons que vos Données sont traitées d'une manière substantiellement équivalente au niveau de protection applicable au sein de l'Union européenne. À cet égard, dans le respect des garanties prévues par le RGPD, vos données sont transférées sur la base de :

- décisions d'adéquation : lorsque le transfert de données personnelles s'effectue vers des pays que la Commission européenne a reconnus comme offrant un niveau de protection adéquat des données personnelles;
- clauses contractuelles types : en l'absence de décisions d'adéquation, nous aurons recours à des contrats spécifiques approuvés par la Commission européenne, visant à garantir le même niveau de protection des données personnelles que celui prévu au sein du territoire européen.

La liste des pays situés en dehors de l'Union européenne vers lesquels Scalapay IP peut transférer vos Données (y compris les informations sur les garanties adoptées) est disponible sur demande, en nous contactant aux coordonnées indiquées dans la présente Politique de Confidentialité.

6. À QUI POUVONS-NOUS COMMUNIQUER VOS DONNÉES PERSONNELLES ?

Au sein de l'organisation de Scalapay IP, les Données pourront être traitées par les agents des services compétents pour l'exécution des différentes activités de traitement.

En outre, afin de fournir nos services, nous pourrions communiquer vos Données Personnelles aux catégories de destinataires énumérés ci-dessous, pour les finalités indiquées, dans le respect des principes de minimisation et de limitation des finalités, et en mettant en œuvre les mesures de sécurité appropriées. En particulier, pour la fourniture des services, les catégories de parties auxquelles nous communiquerons les Données, dans le cadre et dans la limite des finalités poursuivies, sont les suivantes :

- Prestataires : nous pourrions communiquer des Données Personnelles à des prestataires, avec lesquels nous concluons des accords contractuels, que nous utilisons pour vous fournir des services. Parmi ces prestataires et sous-traitants figurent, à titre d'exemple, des fournisseurs de logiciels et de stockage de données, des services de traitement des paiements, des conseillers en affaires.
- Scalapay S.r.l. : Scalapay IP pourrait communiquer vos données personnelles à la société Scalapay S.r.l. en tant qu'opérateur de la Plateforme Scalapay Business sur laquelle vous avez créé un profil.
- Agences KYC (Know-Your-Customer)/AML (Anti-Money Laundering) : dans le cadre des opérations d'intégration (« onboarding ») du Merchant, des vérifications de l'identité de la société et de son bénéficiaire effectif sont effectuées.
- Sociétés et/ou cabinets juridiques de recouvrement de créances : Scalapay IP pourrait avoir la nécessité de partager vos Données afin de procéder au recouvrement de créances échues et impayées.
- Autorités : Scalapay IP pourrait fournir des informations jugées nécessaires aux autorités de police, financières, fiscales ou autres autorités et tribunaux, y compris la Banque d'Italie ou l'Agence des Revenus. Les Données Personnelles sont partagées avec l'autorité lorsque cela est prévu par la loi, dans certains cas à votre demande, ou pour la lutte contre la criminalité. Un exemple d'obligation légale de fournir des informations se présente lorsqu'il est nécessaire d'adopter des mesures contre le blanchiment d'argent et le financement du terrorisme.

Ces entités auront accès aux Données Personnelles nécessaires à l'exercice des fonctions régies par un accord entre les sociétés, et agiront – selon les cas – en qualité de responsables autonomes du traitement ou de sous-traitants (dans ce dernier cas, en vertu d'un accord de désignation en qualité de sous-traitant conformément à l'article 28 du RGPD).

7. PENDANT COMBIEN DE TEMPS UTILISERONS-NOUS VOS DONNÉES PERSONNELLES ?

De plus amples informations sur la durée de conservation de vos données personnelles figurent dans le tableau de la Section 2. Nous conservons vos Données uniquement pour la durée nécessaire à la réalisation des finalités pour lesquelles elles ont été collectées, telles que l'exécution du contrat ou le respect des obligations légales. Lorsque nous décidons de la durée de conservation de vos Données, nous prenons en considération la quantité et le type de Données, leur sensibilité et le risque d'utilisation abusive. Après cette période, vos données seront supprimées ou rendues anonymes.

8. TRAITEMENT DE VÉRIFICATION BIOMÉTRIQUE. ABSENCE DE PRISE DE DÉCISION AUTOMATISÉE

La Société utilise des technologies biométriques pour effectuer la vérification de l'identité des exécutants ou des représentants légaux liés au Merchant qui souhaitent conclure un contrat avec Scalapay IP. Comme indiqué à la Section 2, ce traitement est effectué afin de satisfaire aux obligations légales en matière de prévention du blanchiment d'argent et du financement du terrorisme, telles que requises par la réglementation en matière de lutte contre le blanchiment d'argent (c'est-à-dire le Décret législatif n° 231/2007).

En dehors du cas de la Vérification Alternative (qui, comme indiqué à la Section 4, ne s'applique qu'à titre résiduel), le processus de vérification de l'identité est effectué par des technologies de vérification faciale reposant sur une comparaison individuelle (entre l'image du visage capturée par le selfie ou la vidéo et celle figurant dans le document d'identité fourni). Pour effectuer cette vérification, nous demanderons à l'exécutant ou au représentant légal du Merchant de :

- télécharger une photographie du document d'identité (ou d'un document équivalent) directement sur la Plateforme Scalapay ;
- prendre un selfie ou enregistrer une courte vidéo à l'aide de l'appareil photo du dispositif, en suivant des instructions spécifiques garantissant la bonne acquisition de l'image (par exemple, des conditions d'éclairage adéquates et l'absence d'autres personnes dans le champ).

Nous procéderons à un contrôle des données biométriques de l'exécutant ou du représentant légal du Merchant (le selfie ou la vidéo mentionnés précédemment) pour vérifier la correspondance du visage avec la photographie figurant dans le document d'identité concerné, en vérifiant la cohérence des informations contenues dans le document d'identité avec celles fournies, ainsi que le cadrage et les conditions environnementales. L'exécutant ou le représentant légal du Merchant qui procédera à la vérification biométrique sera en tout état de cause toujours informé de la collecte de la donnée biométrique. De plus, Scalapay IP ne prendra jamais – par le biais du processus décrit ci-dessus – de décisions fondées uniquement sur des traitements automatisés produisant des effets juridiques ou affectant de manière analogue et significative le Merchant. En effet, si la vérification n'aboutit pas, le personnel de la Société sera toujours impliqué pour en évaluer les raisons.

Pour de plus amples informations sur le type de technologie utilisée par la Société et, en tout état de cause, pour exercer ces droits, il est possible de contacter notre délégué à la protection des données (DPO) aux adresses indiquées ci-dessous.

En cas d'utilisation d'outils automatisés pour l'extraction de données à partir de documents d'identité, ces systèmes ne déterminent pas de manière autonome l'issue du processus de vérification, mais soutiennent exclusivement l'activité d'identification, qui est complétée par du personnel autorisé ou par des contrôles supplémentaires.

Les vérifications de l'identité prévoient également un contrôle de la fiabilité de l'image du document fourni, tant par une comparaison entre les vidéos et les images du visage acquises lors du processus d'identification et les images figurant dans le document, que par l'analyse des éléments qui rendent un document d'identité fiable. Ces contrôles sont effectués par un système d'IA, qui n'acquiert pas de données supplémentaires et ne mémorise pas les informations figurant sur les documents. Outre le respect des obligations réglementaires relatives à la correcte identification de la personne concernée, les contrôles ont pour objectif de prévenir d'éventuelles fraudes, pour une meilleure protection des services et

des clients eux-mêmes. Les technologies d'IA utilisées opèrent dans le respect des principes de licéité, de loyauté, de transparence, de proportionnalité et de minimisation des données, et ne conduisent pas à des décisions fondées uniquement sur des traitements automatisés produisant des effets juridiques ou affectant significativement la personne concernée.

9. VOS DROITS

Nous vous rappelons que vous pouvez exercer vos droits relatifs aux données personnelles selon les modalités et dans les limites prévues par les lois sur la protection des données. Vous trouverez ci-après une brève description de ces droits :

- **Droit d'être informé** : toutes les personnes physiques ont le droit d'être informées sur la collecte et l'utilisation de leurs Données Personnelles. Il s'agit d'une exigence fondamentale de transparence telle qu'établie par le RGPD. La présente Politique de Confidentialité et les réponses que nous fournirons à vos demandes satisfont à cette exigence.
- **Droit de demander l'accès aux Données Personnelles** : connu sous le nom de « demande d'accès », il permet d'obtenir la confirmation que des Données font ou ne font pas l'objet d'un traitement et, dans l'affirmative, d'obtenir l'accès aux Données et aux informations mentionnées par le RGPD, ainsi qu'une copie de vos Données Personnelles.
- **Droit de demander la rectification des données personnelles** : il vous permet de corriger et de compléter les éventuelles Données incomplètes ou inexacts en notre possession ; cependant, nous pourrions avoir besoin de vérifier l'exactitude des nouvelles Données fournies.
- **Droit de demander l'effacement des données personnelles (« droit à l'oubli »)** : il vous permet de demander la suppression et l'effacement de vos Données Personnelles lorsqu'il n'existe pas de motifs valables pour continuer à les traiter. Vous pouvez obtenir l'effacement de vos données personnelles dans les cas prévus à l'article 17 du RGPD. Toutefois, nous vous informons que dans certains cas, nous pourrions ne pas être en mesure de satisfaire votre demande d'effacement pour des raisons légales spécifiques (par exemple, lorsque cela est nécessaire pour vous permettre de remplir une obligation légale ou pour constater, exercer ou défendre un droit en justice) qui vous seront communiquées au moment de votre demande.
- **Droit de s'opposer au traitement des données personnelles** : dans les termes prévus à l'article 21 du RGPD, vous pouvez vous opposer au traitement des Données, pour des motifs tenant à votre situation particulière, dans les cas où nous, ou un tiers, nous fondons sur l'intérêt légitime et où vous estimez que ce traitement porte atteinte d'une quelconque manière à vos droits et libertés fondamentaux. Dans ce cas, la Société s'abstiendra de traiter davantage les Données Personnelles, sauf si la Société démontre l'existence de motifs légitimes impérieux pour le traitement qui prévalent sur vos intérêts, droits et libertés, ou pour la constatation, l'exercice ou la défense d'un droit en justice.
- **Droit de demander la limitation du traitement des données personnelles** : vous pouvez demander la limitation du traitement de vos Données Personnelles dans les cas prévus à l'article 18 du RGPD ; nous continuerons à traiter les données personnelles uniquement lorsqu'une exception à cette demande est applicable (par exemple, lorsque le traitement est illicite et que vous vous opposez à l'effacement des Données, en demandant que leur utilisation soit limitée).
- **Droit de demander le transfert des données personnelles vers vous ou vers un tiers (« portabilité des données »)** : nous vous remettons, ou à un tiers que vous aurez désigné, vos Données Personnelles dans un format structuré, couramment utilisé et lisible par machine, dans les conditions prévues à l'article 20 du RGPD. Nous vous rappelons que ce droit s'applique uniquement aux informations traitées par des moyens automatisés et aux traitements effectués sur la base du consentement, ou dans le cadre de l'exécution d'un contrat conclu avec vous.
- **Droit de retirer le consentement à tout moment** : en ce qui concerne les éventuels traitements basés sur votre consentement (tel que recueilli de temps à autre par Scalapay IP après la fourniture d'une politique de

confidentialité appropriée), vous aurez le droit de retirer à tout moment le consentement donné pour les traitements de Données Personnelles basés sur le consentement, et nous cesserons d'utiliser vos données personnelles, sans toutefois affecter la licéité du traitement basé sur le consentement donné avant son retrait.

- **Droit d'introduire une réclamation auprès de l'autorité** : nous vous rappelons que vous avez toujours le droit d'introduire une réclamation auprès de l'Autorité Garante pour la Protection des Données Personnelles, dont le siège est situé Piazza Venezia 11, Rome, à l'adresse e-mail : protocollo@gpdp.it.

10. COOKIES

Scalapay IP n'utilise aucun type de cookie. Cela signifie que lors de votre navigation sur notre site (à l'adresse <https://paymentinstitute.scalapay.com/>), nous ne collectons pas d'informations sur votre dispositif, telles que des données de navigation ou des préférences. Nous n'utilisons pas de cookies tiers à des fins de suivi ou de publicité personnalisée et nous ne partageons pas vos informations avec des tiers par le biais de cookies.

11. CONTACTS

Pour exercer vos droits ou pour demander des informations sur la manière dont nous traitons vos Données Personnelles, vous pouvez nous contacter par e-mail à l'adresse scalapayip@legalmail.it et nous ferons tout notre possible pour vous aider.

En outre, si vous avez des questions relatives au traitement des données personnelles, y compris des demandes d'exercice de vos droits, vous pouvez également contacter notre DPO à l'adresse e-mail suivante : privacy@ip.scalapay.com.