SCALAPAY IP S.P.A. - POLÍTICA DE PRIVACIDAD

Scalapay IP S.p.A., una entidad de pago constituida con arreglo a las leyes de Italia, con domicilio social en Via Nervesa, 21, 20139 Milán (MI), Código Fiscal y número de IVA 06078740484, que ejerce sus actividades de conformidad con los artículos *114-septies* y siguientes del Decreto Legislativo nº 385 de 1 de septiembre de 1993 ("**TUB**"), inscrita en el nº.0 del Registro de Entidades de Pago de conformidad con el art. *114-septies* del Texto Único de la Ley Bancaria ("TUB") y sujeta a la supervisión del Banco de Italia (en lo sucesivo también "**Scalapay IP**" o "**Responsable del Tratamiento**" o "**Sociedad**"), como Responsable del Tratamiento, respeta su privacidad y se compromete a proteger sus datos personales. Scalapay IP se compromete a procesar sus datos de acuerdo con el Reglamento General de Protección de Datos (Reg. UE 2016/679), más conocido como el "**GDPR**", y cualquier otra ley de privacidad aplicable.

Este aviso explica las razones y la forma en que los datos personales se recogen, gestionan y protegen en relación con **los clientes de los servicios de Scalapay IP, también denominados en lo sucesivo Consumidores (SECCIÓN A)**, así como **los vendedores afiliados a Scalapay IP, también denominados en lo sucesivo Comerciantes (SECCIÓN B)**.

En particular, el tratamiento de datos personales realizado por Scalapay IP se ajustará a los principios de licitud, corrección, transparencia, limitación de la finalidad y conservación, minimización de datos, exactitud, integridad y confidencialidad.

Scalapay IP ha designado a un Responsable de la Protección de Datos (el "**Responsable de la Protección de Datos**" o "**RPD**"), con el que los interesados pueden ponerse en contacto para obtener respuestas sobre el tratamiento de datos personales efectuado por el Responsable del Tratamiento, tanto en lo que respecta a los Consumidores como a los Comerciantes, en la siguiente dirección: privacy@ip.scalapay.com.

Es importante que lea esta política, junto con cualquier otra política que podamos proporcionar para complementar, actualizar o ampliar la información relativa a la recogida y tratamiento de sus datos personales. Nos esforzaremos por coordinar estas divulgaciones para que los términos y condiciones aplicados al tratamiento de sus datos personales se presenten siempre de la forma más transparente y fácilmente accesible.

* * *

SECCIÓN A - POLÍTICA DE PRIVACIDAD DEL CONSUMIDOR

1. CONTROLADOR DE DATOS

Este aviso se ha preparado de conformidad con los artículos 13 y 14 del GDPR y tiene por objeto proporcionarle información sobre cómo Scalapay IP procesa sus datos personales como controlador de datos. Sus datos personales se recopilan a través de su uso del sitio web www.scalapay.com y la aplicación Scalapay (en lo sucesivo, la "**Plataforma Scalapay**") cuando decide utilizar uno de los servicios ofrecidos por Scalapay IP, a través de los cuales usted, como consumidor (en lo sucesivo, el "**Consumidor**"), puede adquirir productos y servicios de comerciantes afiliados (en lo sucesivo, los "**Comerciantes**") mediante uno de los servicios de pago (por ejemplo, *Pay in 3, Pay in 4, Pay Later, One-Time Card*, o *pay now-Cart Saver,* mediante tarjeta de un solo uso o BNPL tradicional) ofrecidos por Scalapay IP. Con el fin de ejecutar el contrato celebrado con el Comerciante, Scalapay IP también procesa los Datos recogidos por el Comerciante y/o Scalapay S.r.l..

2. DESCRIPCIÓN DEL TRATAMIENTO

Para facilitar la comprensión de las actividades de tratamiento llevadas a cabo por Scalapay IP, proporcionamos a continuación una tabla que muestra las categorías de datos personales tratados, los fines del tratamiento, la "base jurídica" que autoriza cada tratamiento y lo hace lícito, y el período de tiempo durante el cual Scalapay IP conservará sus datos personales ("**Datos Personales**" o "**Datos**").

Categoría de datos	Finalidad del tratamiento	Base jurídica	Periodo de almacenamiento

Datos de contacto e identificación del consumidor, información sobre bienes/servicios e información de pago. Por ejemplo, nombre, apellidos, código fiscal, dirección residencial (estado, provincia, ciudad, código postal), dirección de envío, lugar de nacimiento, fecha de nacimiento, sexo, dirección de correo electrónico, número de teléfono móvil, nacionalidad, documento de identidad (tipo, número, fecha de expedición, autoridad emisora, ciudad). Detalles de los bienes o servicios adquiridos o pedidos, como el tipo de artículo y el tipo de Comerciante en el que compra	Prestación de servicios de pago a consumidores (*Pay in 3, Pay in 4, Pay Later, One-Time Card*) y, en particular, prestación de las siguientes actividades: - Envío de correos electrónicos relacionados con transacciones - Transmisión de información al Comerciante para la ejecución del contrato - Prestar apoyo en caso de que el consumidor lo solicite	Ejecución de un contrato en el que el consumidor es parte o ejecución de medidas precontractuales adoptadas a petición del consumidor (artículo 6, apartado 1, letra b) del GDPR)	10 (diez) años tras la rescisión del contrato
Datos biométricos del Consumidor (en particular, de los rasgos de la cara del Consumidor tomados del selfie tomado por el Consumidor o del video-selfie tomado por el Consumidor)	Realización de la diligencia debida con el cliente mediante la identificación facial biométrica del consumidor	Obligación legal a la que está sujeto el responsable del tratamiento y la persecución de un interés público (artículo 6, apartado 1, letras c) y e), del GDPR, y artículo 9, apartado 2, letra g), del GDPR, leído en relación con el artículo *2sexies* del Decreto Legislativo 196/2003) a efectos de la legislación contra el blanqueo de capitales y la prevención del fraude, según lo dispuesto expresamente en la legislación pertinente (Decreto Legislativo 231/2007)	10 (diez) años después de la finalización del proceso de diligencia debida
Datos contenidos en el documento de identidad del consumidor y selfie o video-selfie tomada por el		Una obligación legal a la que esté sujeto el Responsable del Tratamiento y la persecución de un interés público (artículo 6,	

consumidor como parte de la verificación.		apartado 1, letras c) y e), del GDPR) a efectos de la legislación contra el blanqueo de capitales y la prevención del fraude, según lo dispuesto expresamente en la legislación pertinente (Decreto Legislativo 231/2007)	
Imagen del rostro del interesado, Datos contenidos en el documento de identidad	Llevar a cabo la diligencia debida con respecto al cliente - a través de la Verificación Alternativa (tal como se define y describe en la Sección 4) - comparando la imagen de la cara del consumidor con la imagen de la cara en el documento de identidad	Una obligación legal a la que esté sujeto el Responsable del Tratamiento y la persecución de un interés público (artículo 6, apartado 1, letras c) y e), del GDPR) a efectos de la legislación contra el blanqueo de capitales y la prevención del fraude, según lo dispuesto expresamente en la legislación pertinente (Decreto Legislativo 231/2007)	10 (diez) años después de la finalización del proceso de diligencia debida
Imágenes y vídeos obtenidos del Consumidor (selfie o video-selfie) y datos contenidos en los documentos de identidad	Realizar controles adicionales de verificación de identidad basados en tecnologías de inteligencia artificial ("IA") aplicadas a las imágenes y vídeos proporcionados por el Consumidor, con el fin de verificar la correspondencia con los documentos de identidad y prevenir fraudes o usos indebidos de los servicios	Una obligación legal a la que esté sujeto el Responsable del Tratamiento y la persecución de un interés público (artículo 6, apartado 1, letras c) y e), del GDPR) a efectos de la legislación contra el blanqueo de capitales y la prevención del fraude, según lo dispuesto expresamente en la legislación pertinente (Decreto Legislativo 231/2007)	10 (diez) años desde la finalización del proceso de diligencia debida o, en cualquier caso, hasta la finalización de las verificaciones de seguridad realizadas mediante IA
Datos identificativos que figuran en el documento de identidad (por ejemplo, nombre, apellidos, fecha y lugar de nacimiento, fecha de expedición y caducidad del documento), recogidos también por medios automatizados en caso de que falle la diligencia debida con el cliente mediante	En caso de que el proceso de reconocimiento biométrico no pueda captar correctamente determinada información del documento de identidad (por ejemplo, las fechas de expedición y caducidad), estos datos pueden ser captados por un sistema de lectura	Una obligación legal a la que esté sujeto el Responsable del Tratamiento y la persecución de un interés público (artículo 6, apartado 1, letras c) y e), del GDPR) a efectos de la legislación contra el blanqueo de capitales y la prevención del fraude,	Los datos se borran al final del proceso de lectura

identificación facial biométrica	automatizada (OCR - Optical Character Recognition).	según lo dispuesto expresamente en la legislación pertinente (Decreto Legislativo 231/2007)	
Datos identificativos que figuran en el documento de identidad (por ejemplo, nombre, apellidos, fecha y lugar de nacimiento, fecha de expedición y caducidad del documento, imagen del rostro)	Verificación documental durante el proceso de diligencia debida mediante un sistema de IA. Análisis automatizado de la imagen del documento (antes de la captura del selfie) para verificar su autenticidad, integridad y posibles signos de falsificación, tras la carga realizada por el Consumidor	Una obligación legal a la que está sujeto el Responsable del Tratamiento y la persecución de un interés público (Artículo 6, apartado 1, letras c) y e) del GDPR) a efectos de la legislación contra el blanqueo de capitales y la prevención del fraude, según lo dispuesto expresamente en la legislación pertinente (Decreto Legislativo 231/2007)	10 (diez) años desde la finalización del proceso de diligencia debida
Datos financieros y de pago (por ejemplo, cuatro últimos dígitos de la tarjeta, fecha de caducidad y lugar de emisión, IBAN)	Procesar el pago de los pedidos y gestionar los cobros y pagos	Ejecución de un contrato en el que el consumidor es parte o ejecución de medidas precontractuales adoptadas a petición del consumidor (artículo 6, apartado 1, letra b) del GDPR)	10 (diez) años tras la rescisión del contrato
	Gestión de AUI (Archivio Unico Informatico), en particular los informes realizados para cumplir las obligaciones reglamentarias y la información al Banco de Italia.	Obligación legal a la que está sujeto el responsable del tratamiento (artículo 6, apartado 1, letra c), del GDPR)	10 (diez) años después de la introducción de la descripción
Datos facilitados voluntariamente por el consumidor	Dar respuesta a las peticiones de los consumidores (por ejemplo, en el caso de una solicitud de apoyo para llevar a cabo la diligencia debida).	Ejecución de un contrato en el que el consumidor es parte o ejecución de medidas precontractuales adoptadas a petición del consumidor (artículo 6, apartado 1, letra b) del GDPR)	Durante el tiempo necesario para proporcionar información al Consumidor y, en cualquier caso, durante un período no superior a 2 (dos) años
Todos los datos personales indicados en este cuadro (excepto los datos biométricos)	Gestión de litigios con los consumidores	Persecución del interés legítimo del responsable del tratamiento en la determinación, el ejercicio o la defensa de un derecho en un	Hasta la conclusión del litigio

		procedimiento judicial o cuando los tribunales ejerzan sus funciones judiciales (artículo 6, apartado 1, letra f)	
Datos de identificación en formato seudonimizado Datos relativos a transacciones ya realizadas utilizando los servicios del Responsable del Tratamiento (importes de las transacciones, fechas de las transacciones y vencimientos de los plazos, estado de los pagos)	Análisis de la integración de la tecnología de Scalapay IP con componentes de terceros para alcanzar los siguientes objetivos: - medición correcta de la solvencia y el riesgo de crédito de los Consumidores que solicitan uno de los instrumentos de pago de la Societad - evaluación correcta de la fiabilidad y puntualidad de los pagos de los Consumidores - prevención del riesgo de fraude, incluida la prevención del riesgo de usurpación de identidad	Scalapay IP trata los datos personales sobre la base de su interés legítimo (artículo 6, apartado 1, letra f) del GDPR). Este tratamiento es necesario para garantizar una gestión responsable de los riesgos, prevenir el fraude y proteger a los Consumidores de un endeudamiento excesivo. El tratamiento ha sido objeto de una ponderación de intereses para garantizar que no menoscaba los derechos y libertades fundamentales del Consumidor. El Consumidor tiene derecho a oponerse a dicho tratamiento en cualquier momento poniéndose en contacto con privacy@ip.scalapay.com	60 días después del análisis de riesgos

3. ENLACES DE TERCEROS

La Plataforma Scalapay, a la que usted accede para realizar compras aplazadas a Comercios, puede incluir enlaces a sitios web de terceros (por ejemplo, los sitios web de los comercios en los que usted adquiere productos o servicios). Al hacer clic o activar dichos enlaces, es posible que terceros procesen sus Datos Personales; por lo tanto, consulte también la política de privacidad de dichos sitios, así como la política de privacidad de la Plataforma Scalapay.

4. SI NO FACILITA SUS DATOS PERSONALES

En algunos casos tenemos que recoger sus datos personales por ley o en virtud de los términos de un contrato que tenemos con usted o estamos tratando de entrar en con usted (por ejemplo, para autorizar el pago aplazado). En estos casos, el hecho de no proporcionar Datos Personales impedirá a Scalapay IP celebrar un contrato con usted.

Más concretamente, para cumplir con la normativa sectorial aplicable a Scalapay IP, el suministro de Datos con fines de verificación biométrica es obligatorio para poder llevar a cabo la verificación de identidad *online*. En cualquier caso, cuando el Consumidor no pueda proceder a la verificación de su identidad en línea debido a limitaciones técnicas del dispositivo, o haya agotado los intentos de verificación de identidad puestos a su disposición por la Sociedad, el Consumidor podrá enviar un correo electrónico a support@scalapay.com adjuntando (i) una foto de un documento de identidad válido (u otro documento equivalente) y (ii) una foto en la que se vea la cara del Consumidor y el documento de identidad que sostiene en la mano. Será responsabilidad del personal de la Sociedad realizar la verificación de identidad ("**Verificación Alternativa**") manualmente. En este caso, no se procesará ningún dato biométrico del Consumidor.

5. TRANSFERENCIAS INTERNACIONALES

Algunos de nuestros proveedores se encuentran fuera de la Unión Europea. Cuando transferimos sus Datos a estos proveedores, nos aseguramos de que sus Datos se procesen y protejan sustancialmente de la misma manera que lo harían en la UE. En este sentido, con sujeción a las salvaguardias establecidas en el GDPR, sus Datos se transfieren sobre la base de:

- decisiones de adecuación: cuando la transferencia de datos personales tiene lugar a países que la Comisión Europea ha considerado que ofrecen un nivel adecuado de protección de datos personales;
- cláusulas contractuales tipo: en ausencia de decisiones de adecuación, utilizaremos contratos específicos aprobados por la Comisión Europea para garantizar la misma protección de los datos personales que en el territorio europeo.

La lista de países fuera de la Unión Europea a los que Scalapay IP puede transferir sus datos (incluida la información sobre las medidas de protección aplicadas) está disponible previa solicitud poniéndose en contacto con nosotros en los datos de contacto que figuran en esta política.

6. ¿A QUIÉN PODEMOS REVELAR SUS DATOS PERSONALES?

Dentro de la organización Scalapay IP, los datos podrán ser tratados por los responsables de las oficinas encargadas de llevar a cabo las actividades individuales de tratamiento.

Además, con el fin de prestarle nuestros servicios, podemos revelar sus Datos Personales a las categorías de destinatarios que se enumeran a continuación, para los fines que se enumeran a continuación, de conformidad con los principios de minimización y limitación de la finalidad, y tomando las medidas de seguridad adecuadas. Los destinatarios exactos a los que revelaremos sus Datos Personales dependerán de los servicios que utilice. En particular, para la prestación de los servicios, las categorías de personas a las que revelaremos Datos, en razón y en la medida de las finalidades perseguidas, son:

- Proveedores: podemos revelar Datos Personales a proveedores -con los que celebramos acuerdos contractuales- que utilizamos para prestarle servicios. Ejemplos de estos proveedores son los proveedores de software y almacenamiento de datos, los servicios de procesamiento de pagos, los consultores empresariales, las empresas que proporcionan software de escaneado facial biométrico a los consumidores y las empresas de *redes afiliadas*.
- Augusta SPV S.r.l.: Scalapay IP puede revelar sus Datos Personales a la empresa Augusta SPV s.r.l., un vehículo para la titulización de créditos de conformidad con la ley nº 130 de 30 de abril de 1999, ya que participa en la operación de titulización para el suministro de instrumentos de pago a los Consumidores.
- Scalapay S.r.l.: Scalapay IP podrá comunicar sus Datos Personales a Scalapay S.r.l. como titular de la Plataforma Scalapay en la que usted ha creado un perfil de usuario.
- Tiendas online y físicas: Scalapay IP puede revelar Información Personal a la tienda online en la que usted realice una compra. Esto se hace con el fin de permitir a la tienda administrar su compra y su relación con la tienda, enviarle mercancía, manejar disputas y prevenir el fraude. Cualquier dato personal que proporcione a una tienda estará sujeto a la política de privacidad de la tienda.
- Proveedores de servicios de pago ("**PSP**"): los PSP permiten aceptar pagos electrónicos a través de una amplia gama de métodos de pago, como tarjetas de crédito, pagos bancarios como adeudos domiciliados, etc.
- Empresas de cobro de deudas: Scalapay IP puede necesitar compartir sus Datos cuando vende o subcontrata el cobro de deudas vencidas e impagadas a un tercero, como una empresa de cobro de deudas.
- Empresas que evalúan la solvencia crediticia de los consumidores: Con el fin de garantizar una correcta evaluación crediticia y la seguridad de las transacciones, Scalapay IP puede compartir determinados datos con terceros asociados, incluida la empresa Qlarifi Limited. Los datos compartidos pueden incluir información

sobre transacciones realizadas, datos de identificación del consumidor e historial de pagos. Qlarifi procesa estos datos únicamente con fines de scoring y prevención del fraude, de conformidad con los acuerdos de procesamiento de datos existentes.

- Autoridades: Scalapay IP puede proporcionar la información que considere necesaria a las autoridades policiales, financieras, fiscales o de otro tipo y los tribunales, incluido el Banco de Italia o el Servicio de Impuestos Internos. Compartiremos Información Personal con las autoridades si así lo exige la ley, en algunos casos a petición suya, o si es necesario para la administración de deducciones fiscales, para combatir el crimen o para proteger nuestros derechos en procedimientos judiciales o extrajudiciales. Un ejemplo de obligación legal de facilitar información es cuando es necesario tomar medidas contra el blanqueo de dinero y la financiación del terrorismo.

Estas entidades tendrán acceso a los Datos Personales necesarios para desempeñar las funciones reguladas por un acuerdo entre las empresas, y actuarán -según el caso- como controladores o procesadores de datos autónomos (en este último caso, en virtud de un acuerdo que los designe como procesadores de datos de conformidad con el artículo 28 del GDPR).

7. ¿DURANTE CUÁNTO TIEMPO UTILIZAREMOS SUS DATOS?

Encontrará más información sobre el periodo de conservación en la tabla de la sección 2. Sólo conservamos sus Datos durante el tiempo necesario para alcanzar los fines para los que los recogimos, como la ejecución de un contrato o el cumplimiento de obligaciones legales. A la hora de decidir durante cuánto tiempo conservamos sus Datos, tenemos en cuenta la cantidad y el tipo de Datos, su sensibilidad y el riesgo de uso indebido.

Al final del periodo de conservación, los Datos Personales se suprimirán o anonimizarán. Por lo tanto, al expirar este periodo, el interesado no podrá ejercer los derechos establecidos en la sección 9 (como el derecho de acceso, supresión, rectificación y portabilidad de los Datos Personales).

8. TRATAMIENTO DE VERIFICACIÓN BIOMÉTRICA. NINGÚN PROCESO AUTOMATIZADO DE TOMA DE DECISIONES

La Sociedad utiliza tecnologías biométricas para verificar la identidad de los Consumidores que desean utilizar los servicios de pago ofrecidos por Scalapay IP. Como se indica en la sección 2dicho tratamiento se lleva a cabo con el fin de cumplir con las obligaciones legales relativas a la prevención del blanqueo de capitales y la financiación del terrorismo, tal y como exige la legislación contra el blanqueo de capitales (incluido el Decreto Legislativo 231/2007).

Fuera de la hipótesis de verificación alternativa (que, como se indica en la sección 4 sólo se aplica en casos residuales), el proceso de verificación de identidad se lleva a cabo a través de tecnologías de verificación facial que se basan en una comparación *uno a uno* (entre la imagen de su rostro captada por el selfie o vídeo y la imagen que figura en el documento de identidad que usted facilita). Para llevar a cabo dicha verificación, le pediremos:

- cargar una fotografía de su documento de identidad (u otro documento equivalente) directamente en la Plataforma Scalapay;
- hazte un selfie o graba un vídeo corto a través de la cámara de tu dispositivo, siguiendo instrucciones específicas para garantizar que la imagen se captura correctamente (por ejemplo, condiciones de iluminación adecuadas y ninguna otra persona en el encuadre);

Realizaremos un cribado de sus datos biométricos (el selfie o vídeo antes mencionado) para verificar la correspondencia de su rostro con la fotografía del documento de identidad correspondiente, comprobando la coherencia de la información incluida en el documento de identidad con la facilitada por usted, así como el encuadre y las condiciones ambientales. Siempre será consciente de la recogida de datos biométricos. Pero eso no es todo: Scalapay IP nunca -a través del proceso que acabamos de describir- tomará decisiones basadas únicamente en un tratamiento automatizado que produzcan efectos jurídicos o le afecten significativamente de forma similar. De hecho, en caso de que la verificación falle, el personal de la empresa siempre intervendrá para evaluar las razones de ello.

Para más información sobre el tipo de tecnología utilizada por la Sociedad y, en cualquier caso, para ejercer estos derechos, puede ponerse en contacto con nuestro Responsable de Protección de Datos en las direcciones indicadas a continuación.

Cuando se utilizan herramientas automatizadas para extraer datos de los documentos de identidad, estos sistemas no determinan de forma independiente el resultado del proceso de verificación, sino que sólo sirven de apoyo a la actividad de identificación, que es completada por personal autorizado o controles adicionales.

Los procedimientos de verificación de identidad también incluyen una comprobación de la fiabilidad de la imagen del documento proporcionado, realizada tanto mediante una comparación entre los vídeos e imágenes faciales recopilados durante el proceso de identificación y las imágenes contenidas en el documento, como mediante el análisis de los elementos que hacen fiable un documento de identidad. Estas comprobaciones se llevan a cabo mediante un sistema de inteligencia artificial (IA), que no recopila datos adicionales ni almacena la información contenida en los documentos. Además de cumplir con las obligaciones legales relativas a la correcta identificación del interesado, estas comprobaciones tienen como objetivo prevenir posibles fraudes, garantizando así una mayor protección de los servicios y de los propios clientes. Las tecnologías de IA empleadas operan en cumplimiento de los principios de licitud, lealtad, transparencia, proporcionalidad y minimización de datos, y no dan lugar a decisiones basadas únicamente en tratamientos automatizados que produzcan efectos jurídicos o afecten significativamente al interesado.

9. SUS DERECHOS

Le recordamos que puede ejercer sus derechos relativos a sus datos personales en la forma y dentro de los límites previstos por las leyes de protección de datos. A continuación encontrará una breve descripción de estos derechos que puede ejercer en las condiciones del GDPR:

- **Derecho a ser informado**: todas las personas tienen derecho a ser informadas sobre la recogida y el uso de sus Datos Personales. Se trata de un requisito fundamental de transparencia establecido en el GDPR. El presente aviso y las respuestas que proporcionamos a sus consultas cumplen este requisito.

- **Derecho a solicitar el acceso a los Datos Personales**: conocido como "solicitud de acceso", le permite obtener confirmación sobre si los Datos se están procesando o no y, en caso afirmativo, obtener acceso a los Datos y a la información mencionada en el GDPR, así como obtener una copia de sus Datos Personales.

- **Derecho a solicitar la rectificación de datos personales**: le permite corregir y completar cualquier dato incompleto o inexacto que tengamos; sin embargo, es posible que tengamos que verificar la exactitud de los nuevos datos facilitados.

- **Derecho a solicitar la supresión de sus Datos Personales ("derecho al olvido")**: le permite solicitar la supresión y eliminación de sus Datos Personales cuando no existan motivos válidos para seguir tratándolos. Puede obtener la supresión de sus Datos Personales en los casos previstos en el artículo 17 del GDPR. Sin embargo, tenga en cuenta que en ciertos casos es posible que no podamos cumplir con su solicitud de eliminación por razones legales específicas (por ejemplo, cuando sea necesario para permitirle cumplir con una obligación legal o para establecer, ejercer o defender un derecho ante un tribunal) que se le comunicará en el momento de su solicitud.

- **Derecho a oponerse al tratamiento de sus Datos Personales**: en virtud de lo dispuesto en el artículo 21 del GDPR, podrá oponerse al tratamiento de sus Datos Personales, por motivos relacionados con su situación particular, en los casos en que nosotros, o un tercero, nos basemos en un interés legítimo y si considera que dicho tratamiento vulnera de algún modo sus derechos y libertades fundamentales. En tal caso, la Sociedad se abstendrá de seguir tratando sus Datos Personales a menos que la Sociedad pueda demostrar motivos legítimos imperiosos para el tratamiento que prevalezcan sobre sus intereses, derechos y libertades o para el establecimiento, ejercicio o defensa de reclamaciones legales. Para ejercer este derecho, puede ponerse en contacto con nosotros en privacy@ip.scalapay.com.

- **Derecho a solicitar la limitación del tratamiento de** datos personales: puede solicitar la limitación del tratamiento de sus datos personales en los casos previstos en el artículo 18 del GDPR (por ejemplo, si el tratamiento es ilícito y se opone a la supresión de los Datos, solicitando que se restrinja su uso).

- **Derecho a solicitar la transferencia de sus Datos Personales a usted o a un tercero ("portabilidad de datos")**: le entregaremos sus Datos Personales a usted o a un tercero delegado por usted en un formato estructurado,

de uso común y lectura mecánica, en las condiciones establecidas en el artículo 20 del GDPR. Tenga en cuenta que este derecho sólo se aplica a la información tratada por medios automatizados y para el tratamiento que tiene lugar sobre la base del consentimiento, o como parte de la ejecución de un contrato celebrado con usted.

- **Derecho a revocar el consentimiento en cualquier momento**: limitado a cualquier tratamiento basado en su consentimiento (recogido de vez en cuando por Scalapay IP tras la provisión de la notificación pertinente) usted tendrá derecho a revocar su consentimiento para el tratamiento de Datos Personales basado en su consentimiento en cualquier momento y dejaremos de utilizar sus Datos Personales, pero sin perjuicio de la legalidad del tratamiento basado en su consentimiento antes de la revocación.
- **Derecho a presentar** una reclamación ante la autoridad: le recordamos que siempre tiene derecho a presentar una reclamación ante la Autoridad Italiana de Protección de Datos, con sede en Piazza Venezia 11, Roma, en la siguiente dirección de correo electrónico: protocollo@gpdp.it.

10. COOKIE

Scalapay IP no utiliza ningún tipo de cookies en su sitio institucional (https://paymentinstitute.scalapay.com/). Esto significa que mientras navega por nuestro sitio, no recopilamos ninguna información en su dispositivo, como datos de navegación o preferencias. No utilizamos cookies de terceros para el seguimiento o publicidad personalizada y no compartimos su información con terceros mediante el uso de cookies.

11. CONTACTOS

Para ejercer sus derechos o solicitar información sobre cómo procesamos sus Datos Personales, puede ponerse en contacto con nosotros por correo electrónico en scalapayip@legalmail.it y haremos todo lo posible por ayudarle.

Además, si tiene alguna pregunta relativa al tratamiento de Datos Personales, incluidas las solicitudes para ejercer sus derechos, también puede ponerse en contacto con nuestro RPD utilizando la siguiente dirección de correo electrónico: privacy@ip.scalapay.com.

* * *

SECCIÓN B – POLÍTICA DE PRIVACIDAD DEL COMERCIANTE

1. CONTROLADOR DE DATOS

Este aviso se prepara de conformidad con los artículos 13 y 14 del GDPR y tiene por objeto proporcionarle información sobre cómo Scalapay IP procesa sus datos personales. Sus datos personales han sido recogidos por Scalapay S.r.l. a través de su uso del sitio web www.scalapay.com y la plataforma de negocios (en adelante, la "**Plataforma de Negocios Scalapay**") o por Scalapay IP cuando usted firma un contrato con Scalapay IP como comerciante afiliado (en adelante, el "**Comerciante**") con el fin de ofrecer a sus clientes uno de los servicios de pago (por ejemplo, *Pay in 3*, *Pay in 4, Pay Later, One-Time Card,* o *Pay now-Cart Saver* a través de tarjeta de pago único o BNPL tradicional) ofrecidos por Scalapay IP.

2. DESCRIPCIÓN DEL TRATAMIENTO

Para facilitar la comprensión de las actividades de tratamiento llevadas a cabo por Scalapay IP, proporcionamos a continuación una tabla que muestra las categorías de datos personales tratados, los fines del tratamiento, la "base jurídica" que autoriza cada tratamiento y lo hace lícito, y el período de tiempo durante el cual Scalapay IP conservará sus datos personales ("**Datos Personales**" o "**Datos**").

Categoría de datos	**Finalidad del tratamiento**	**Base jurídica**	**Periodo de almacenamiento**
Datos de contacto e identificación del Comerciante (por ejemplo, nombre, apellidos, dirección de correo electrónico y número de teléfono de la empresa de los empleados del Comerciante)	- Ejecución del contrato firmado con el Comerciante - Creación y gestión de perfiles de Comerciantes en la plataforma empresarial Scalapay	Ejecución de un contrato en el que el interesado sea parte o ejecución de medidas precontractuales adoptadas a petición del interesado (artículo 6, apartado 1, letra b), del GDPR)	Durante 10 (diez) años tras la finalización de la relación contractual
Datos biométricos del ejecutor o representante legal del Comerciante (en particular, a partir de las características faciales del ejecutor o representante legal extraídas de la selfie tomada por el ejecutor o representante legal o de la videosefie realizada por este).	Realización de la diligencia debida con el Comerciante	Obligación legal a la que está sujeto el responsable del tratamiento y la persecución de un interés público (artículo 6, apartado 1, letras c) y e), del GDPR, y artículo 9, apartado 2, letra g), del GDPR, leído en relación con el artículo *2sexies* del Decreto Legislativo 196/2003) a efectos de la legislación contra el blanqueo de capitales y la prevención del fraude, según lo dispuesto expresamente en la legislación pertinente (Decreto Legislativo 231/2007)	10 (diez) años después de la finalización del proceso de diligencia debida

Datos contenidos en el documento de identidad del ejecutor o del representante legal del Comerciante y selfie o video-selfie realizado por este en el marco de la verificación		Obligación legal a la que está sujeto el Responsable del Tratamiento (artículo 6, apartado 1, letra c), del GDPR) a efectos de la legislación contra el blanqueo de capitales y para prevenir el fraude, según lo dispuesto expresamente en la legislación sectorial (Decreto Legislativo 231/2007)	
-Imagen del rostro, del ejecutor o del representante legal del Comerciante -Datos contenidos en el documento de identidad	Realizar la diligencia debida con el Comerciante, mediante Verificación Alternativa (como se define y describe en la Sección 4), comparando la imagen del rostro del ejecutor o representante legal del Comerciante con la imagen del rostro que aparece en el documento de identidad.	Obligación legal a la que está sujeto el Responsable del Tratamiento (artículo 6, apartado 1, letra c), del GDPR) a efectos de la legislación contra el blanqueo de capitales y para prevenir el fraude, según lo dispuesto expresamente en la legislación sectorial (Decreto Legislativo 231/2007)	10 (diez) años después de la finalización del proceso de diligencia debida
Imágenes y vídeos obtenidos del ejecutor o representante legal del Comerciante (selfie o video-selfie) y datos contenidos en los documentos de identidad	Realizar controles adicionales de verificación de identidad basados en tecnologías de inteligencia artificial ("IA") aplicadas a las imágenes y vídeos proporcionados, con el fin de reforzar la verificación de la correspondencia con los documentos de identidad y prevenir fraudes o usos indebidos de los servicios	Una obligación legal a la que esté sujeto el Responsable del Tratamiento y la persecución de un interés público (artículo 6, apartado 1, letras c) y e), del GDPR) a efectos de la legislación contra el blanqueo de capitales y la prevención del fraude, según lo dispuesto expresamente en la legislación pertinente (Decreto Legislativo 231/2007)	10 (diez) años desde la finalización del proceso de diligencia debida o, en cualquier caso, hasta la finalización de las verificaciones de seguridad realizadas mediante IA
Datos identificativos que figuran en el documento de identidad del ejecutor o del representante legal del Comerciante (por ejemplo, nombre, apellidos, fecha y lugar de nacimiento, fecha de expedición y caducidad del documento), recogidos también por medios automatizados en caso de que falle la diligencia debida del ejecutor o del representante legal del Comerciante mediante identificación facial biométrica	En caso de que el proceso de diligencia debida con el Comerciante no pueda captar correctamente determinada información del documento de identidad (por ejemplo, las fechas de expedición y caducidad), estos datos pueden ser captados por un sistema de lectura automatizada (OCR -	Obligación legal a la que esté sujeto el Responsable del Tratamiento y la persecución de un interés público (artículo 6, apartado 1, letras c) y e), del GDPR) a efectos de la legislación contra el blanqueo de capitales y la prevención del fraude, según lo dispuesto expresamente en la legislación pertinente (Decreto Legislativo 231/2007)	Los datos se borran al final del proceso de lectura

	Optical Character Recognition)		
Datos identificativos que figuran en el documento de identidad (por ejemplo, nombre, apellidos, fecha y lugar de nacimiento, fecha de expedición y caducidad del documento, imagen del rostro)	Verificación documental durante el proceso de diligencia debida mediante un sistema de inteligencia artificial. Análisis automatizado de la imagen del documento (antes de la captura del selfie) para verificar su autenticidad, integridad y posibles signos de falsificación, tras la carga realizada por el Consumidor	Una obligación legal a la que está sujeto el Responsable del Tratamiento y la persecución de un interés público (Artículo 6, apartado 1, letras c) y e) del GDPR) a efectos de la legislación contra el blanqueo de capitales y la prevención del fraude, según lo dispuesto expresamente en la legislación pertinente (Decreto Legislativo 231/2007)	10 (diez) años desde la finalización del proceso de diligencia debida
Datos personales relativos a empleados y/o colaboradores del Comerciante facilitados voluntariamente	Prestar apoyo al Comerciante	ejecución de un contrato en el que el interesado sea parte o ejecución de medidas precontractuales adoptadas a petición del interesado (artículo 6, apartado 1, letra b), del GDPR)	Durante el tiempo necesario para proporcionar información al interesado y, en cualquier caso, durante un período no superior a 2 (dos) años.

3. ENLACES DE TERCEROS

La plataforma empresarial Scalapay no incluye enlaces a sitios web de terceros.

4. SI NO FACILITA SUS DATOS PERSONALES

En algunos casos tenemos que recoger sus datos personales por ley o en virtud de los términos de un contrato que tenemos con usted o estamos tratando de entrar en con usted. En estos casos, el hecho de no proporcionar sus Datos Personales impedirá a Scalapay IP celebrar un contrato con usted y/o prestarle el servicio.

Más concretamente, para cumplir con la normativa sectorial aplicable a la Sociedad, la aportación de Datos con fines de verificación biométrica es obligatoria para que podamos llevar a cabo la verificación de la identidad en línea. En cualquier caso, si el representante legal o el ejecutor del Comerciante no puede proceder a la verificación de su identidad en línea debido a limitaciones técnicas del dispositivo, o si ha agotado los intentos de verificación de identidad proporcionados por la empresa, el representante legal o el ejecutor del Comerciante puede enviar un correo electrónico a la dirección support@scalapay. com adjuntando (i) una foto del documento de identidad en vigor (u otro documento equivalente) y (ii) una foto en la que se vea el rostro del representante legal o albacea del Comerciante y el documento de identidad que se sostiene en la mano. El personal de la empresa se encargará de verificar manualmente la identidad ("**Verificación Alternativa**"). En tal caso, no se tratarán datos biométricos del representante legal o ejecutor del Comerciante.

5. TRANSFERENCIAS INTERNACIONALES

Algunos de nuestros proveedores se encuentran fuera de la Unión Europea. Cuando transferimos sus Datos a estos proveedores, nos aseguramos de que sus Datos sean tratados sustancialmente de la misma manera que lo serían en la UE. En este sentido, con sujeción a las salvaguardias establecidas en el GDPR, sus Datos se transfieren sobre la base de:

- decisiones de adecuación: cuando se transfieren datos personales a países que la Comisión Europea ha considerado que ofrecen un nivel adecuado de protección de datos personales;
- cláusulas contractuales tipo: en ausencia de decisiones de adecuación, utilizaremos contratos específicos aprobados por la Comisión Europea para garantizar la misma protección de los datos personales que en el territorio europeo.

La lista de países fuera de la Unión Europea a los que Scalapay IP puede transferir sus datos (incluida la información sobre las medidas de protección aplicadas) está disponible previa solicitud poniéndose en contacto con nosotros en los datos de contacto que figuran en esta política.

6. ¿A QUIÉN PODEMOS REVELAR SUS DATOS PERSONALES?

Dentro de la organización Scalapay IP, los datos podrán ser tratados por los responsables de las oficinas encargadas de llevar a cabo las actividades individuales de tratamiento.

Además, para la prestación de nuestros servicios, podremos revelar sus Datos Personales a las categorías de destinatarios que se indican a continuación, para las finalidades que se indican a continuación, de conformidad con los principios de minimización y limitación de la finalidad, y adoptando las medidas de seguridad adecuadas. En particular, para la prestación de servicios, las categorías de destinatarios a los que revelaremos Datos, en razón y en la medida de las finalidades perseguidas, son:

- Proveedores: podemos revelar Datos Personales a proveedores, con los que celebramos acuerdos contractuales, que utilizamos para prestarle servicios. Ejemplos de estos proveedores y subcontratistas son los proveedores de software y almacenamiento de datos, los servicios de procesamiento de pagos y los consultores empresariales.
- Scalapay S.r.l.: Scalapay IP puede comunicar sus datos personales a la empresa Scalapay S.r.l. como propietaria de la Plataforma de Negocios Scalapay donde usted ha creado un perfil.
- Agencias KYC (*Know-Your-Customer*)/AML *(Anti-Money Laundering*): en el marco de las operaciones de "*onboarding*" del C omerciante, se efectúan comprobaciones sobre la identidad de la empresa y del beneficiario efectivo.
- Empresas de cobro de deudas y/o bufetes de abogados: Scalapay IP puede necesitar compartir sus datos para llevar a cabo actividades de cobro de deudas vencidas e impagadas.
- Autoridades: Scalapay IP puede proporcionar la información que considere necesaria a las autoridades policiales, financieras, fiscales o de otro tipo y los tribunales, incluido el Banco de Italia o el Servicio de Impuestos Internos. Los datos personales se comparten con la autoridad si es requerido por la ley, en algunos casos a petición suya, o para fines policiales. Un ejemplo de obligación legal de facilitar información es cuando es necesario tomar medidas contra el blanqueo de dinero y la financiación del terrorismo.

Estas entidades tendrán acceso a los Datos Personales necesarios para desempeñar las funciones reguladas por un acuerdo entre las empresas, y actuarán -según el caso- como controladores o procesadores de datos autónomos (en este último caso, en virtud de un acuerdo que los designe como procesadores de datos de conformidad con el artículo 28 del GDPR).

7. ¿DURANTE CUÁNTO TIEMPO UTILIZAREMOS SUS DATOS?

Puede encontrar más información sobre el periodo de conservación en la tabla de la sección 2. Sólo conservamos sus Datos durante el tiempo necesario para alcanzar los fines para los que los recopilamos, como la ejecución del contrato o el cumplimiento de obligaciones legales. Cuando decidimos cuánto tiempo conservar sus Datos, tenemos en cuenta la cantidad y el tipo de Datos, su sensibilidad y el riesgo de uso indebido. Transcurrido este plazo, sus datos se eliminarán o se convertirán en anónimos.

8. TRATAMIENTO DE VERIFICACIÓN BIOMÉTRICA. AUSENCIA DE PROCESO DECISORIAL AUTOMATIZADO

La Sociedad utiliza tecnologías biométricas para verificar la identidad de los ejecutores o representantes legales vinculados al Comerciante que deseen celebrar un contrato con Scalapay IP. Como se indica en la Sección 2, este tratamiento se lleva a cabo para cumplir con las obligaciones legales en materia de prevención del blanqueo de capitales y la financiación del terrorismo, tal y como exige la normativa contra el blanqueo de capitales (incluida el Decreto Legislativo 231/2007).

Fuera de la hipótesis de la Verificación Alternativa (que, como se indica en la sección 4, se aplica exclusivamente en casos residuales), el proceso de verificación de la identidad se lleva a cabo mediante tecnologías de verificación facial que se basan en la comparación uno a uno (entre la imagen del rostro capturada por la selfie o el vídeo y la que aparece en el documento de identidad proporcionado). Para llevar a cabo dicha verificación, pediremos al ejecutor o representante legal del Comerciante que:

- cargar una fotografía del documento de identidad (u otro documento equivalente) directamente en la Plataforma Scalapay;
- tomar un selfie o grabar un breve vídeo con la cámara del dispositivo, siguiendo instrucciones específicas que garanticen la correcta captura de la imagen (por ejemplo, condiciones de iluminación adecuadas y ausencia de otras personas en el encuadre);

Realizaremos un examen de los datos biométricos del ejecutor o representante legal del Comerciante (el selfie o el vídeo mencionados anteriormente) para verificar la correspondencia del rostro con la fotografía del documento de identidad correspondiente, verificando la coherencia de la información incluida en el documento de identidad con la que se debe proporcionar, así como el encuadre y las condiciones ambientales. El ejecutor o representante legal del Comerciante que llevará a cabo la verificación biométrica siempre será consciente de la recopilación de datos biométricos. Pero no solo eso: Scalapay IP nunca tomará - a través del proceso recién descrito - decisiones basadas únicamente en tratamientos automatizados que produzcan efectos jurídicos o afecten significativamente de manera similar al Comerciante. De hecho, si la verificación no tiene éxito, el personal de la empresa siempre participará en la evaluación de las razones.

Para obtener más información sobre el tipo de tecnología utilizada por la empresa y, en cualquier caso, para ejercer estos derechos, puede ponerse en contacto con nuestro delegado de protección de datos (DPO) en las direcciones que se indican a continuación.

Cuando se utilizan herramientas automatizadas para extraer datos de los documentos de identidad, estos sistemas no determinan de forma independiente el resultado del proceso de verificación, sino que sólo sirven de apoyo a la actividad de identificación, que es completada por personal autorizado o controles adicionales.

Los procedimientos de verificación de identidad también incluyen una comprobación de la fiabilidad de la imagen del documento proporcionado, realizada tanto mediante una comparación entre los vídeos e imágenes faciales recopilados durante el proceso de identificación y las imágenes contenidas en el documento, como mediante el análisis de los elementos que hacen fiable un documento de identidad. Estas comprobaciones se llevan a cabo mediante un sistema de inteligencia artificial (IA), que no recopila datos adicionales ni almacena la información contenida en los documentos. Además de cumplir con las obligaciones legales relativas a la correcta identificación del interesado, estas comprobaciones tienen como objetivo prevenir posibles fraudes, garantizando así una mayor protección de los servicios y de los propios clientes. Las tecnologías de IA empleadas operan en cumplimiento de los principios de licitud, lealtad, transparencia, proporcionalidad y minimización de datos, y no dan lugar a decisiones basadas únicamente en tratamientos automatizados que produzcan efectos jurídicos o afecten significativamente al interesado.

9. SUS DERECHOS

Le recordamos que puede ejercer sus derechos relativos a sus datos personales en la forma y dentro de los límites previstos por la legislación sobre protección de datos. A continuación encontrará una breve descripción de estos derechos:

- **Derecho a ser informado**: todas las personas tienen derecho a ser informadas sobre la recogida y el uso de sus Datos Personales. Se trata de un requisito fundamental de transparencia establecido en el GDPR. El presente Aviso y las respuestas que proporcionamos a sus consultas cumplen este requisito.

- **Derecho a solicitar el acceso a los Datos Personales**: conocido como "solicitud de acceso", le permite obtener confirmación sobre si los Datos se están procesando o no y, en caso afirmativo, obtener acceso a los Datos y a la información mencionada en el GDPR, así como obtener una copia de sus Datos Personales.

- **Derecho a solicitar la rectificación de los datos personales**: le permite corregir y completar los Datos incompletos o inexactos que obren en nuestro poder; no obstante, es posible que tengamos que verificar la exactitud de los nuevos Datos facilitados.

- **Derecho a solicitar la supresión de datos personales ("derecho al olvido")**: le permite solicitar la supresión y eliminación de sus Datos Personales cuando no exista una razón válida para seguir tratándolos. Puede obtener la supresión de sus Datos Personales en los casos previstos en el artículo 17 del GDPR. No obstante, tenga en cuenta que, en determinados casos, es posible que no podamos acceder a su solicitud de supresión por motivos legales específicos (por ejemplo, cuando sea necesario para permitirle cumplir con una obligación legal o para establecer, ejercer o defender un derecho ante un tribunal) que se le comunicarán en el momento de su solicitud.

- **Derecho a oponerse al tratamiento de sus Datos Personales**: en virtud de lo dispuesto en el artículo 21 del GDPR, podrá oponerse al tratamiento de sus Datos Personales, por motivos relacionados con su situación particular, en los casos en que nosotros, o un tercero, nos basemos en un interés legítimo y si considera que dicho tratamiento vulnera de algún modo sus derechos y libertades fundamentales. En tal caso, la Sociedad se abstendrá de seguir tratando sus Datos Personales a menos que la Sociedad pueda demostrar motivos legítimos imperiosos para el tratamiento que prevalezcan sobre sus intereses, derechos y libertades o para el establecimiento, ejercicio o defensa de reclamaciones legales.

- **Derecho a solicitar la limitación del tratamiento de sus Datos Personales**: usted puede solicitar la limitación del tratamiento de sus Datos Personales en los casos previstos en el artículo 18 GDPR, continuaremos tratando sus Datos Personales sólo si es aplicable una excepción a esta solicitud (por ejemplo, en el caso de que el tratamiento sea ilícito y usted se oponga a la supresión de los Datos, solicitando la limitación de su uso).

- **Derecho a solicitar la transferencia de datos personales a usted o a un tercero ("portabilidad de datos")**: le entregaremos sus Datos Personales a usted o a una parte delegada por usted en un formato estructurado, de uso común y lectura mecánica, en las condiciones establecidas en el artículo 20 del GDPR. Tenga en cuenta que este derecho sólo se aplica a la información tratada por medios automatizados y para el tratamiento que tiene lugar sobre la base del consentimiento, o como parte de la ejecución de un contrato celebrado con usted.

- **Derecho a revocar el consentimiento en cualquier momento**: limitado a cualquier tratamiento basado en su consentimiento (recogido de vez en cuando por Scalapay IP tras la provisión de la notificación pertinente) usted tendrá derecho a revocar su consentimiento para el tratamiento de Datos Personales basado en su consentimiento en cualquier momento y dejaremos de utilizar sus Datos Personales, pero sin perjuicio de la legalidad del tratamiento basado en su consentimiento antes de la revocación.

- **Derecho a presentar** una reclamación ante la autoridad: le recordamos que siempre tiene derecho a presentar una reclamación ante la Autoridad Italiana de Protección de Datos, con sede en Piazza Venezia 11, Roma, en la siguiente dirección de correo electrónico: protocollo@gpdp.it.

10. COOKIE

Scalapay IP no utiliza ningún tipo de cookies. Esto significa que cuando navegas por nuestra web (en el enlace https://paymentinstitute.scalapay.com/), no recogemos ninguna información de tu dispositivo, como datos de navegación o preferencias. No utilizamos cookies de terceros para el seguimiento o publicidad personalizada y no compartimos su información con terceros mediante el uso de cookies.

11. CONTACTOS

Para ejercer sus derechos o solicitar información sobre cómo tratamos sus Datos Personales, puede ponerse en contacto con nosotros por correo electrónico en scalapayip@legalmail.it y haremos todo lo posible por ayudarle.

Además, si tiene alguna pregunta sobre el tratamiento de datos personales, incluidas las solicitudes para ejercer sus derechos, también puede ponerse en contacto con nuestro RPD a través de la siguiente dirección de correo electrónico: privacy@ip.scalapay.com.