ANEXO SOBRE PROTECCIÓN DE DATOS

El presente Anexo sobre el Tratamiento de Datos («**DPA**» o «**Anexo**») forma parte del contrato de servicios entre («Planet») y (el «Comerciante») con fecha (el **«Contrato**»).

Planet y el Comerciante (denominados individualmente «**Parte**» y conjuntamente «**Partes**») acuerdan que el presente DPA establece los requisitos de protección de datos que se aplican al tratamiento de Datos personales (o Datos personales compartidos, según corresponda) por parte de las Partes para los fines establecidos en el Contrato y/o en el presente DPA.

1. Definiciones

Las siguientes definiciones se aplican en este Anexo:

1.1. **Afiliados**: cualquier persona física, sociedad, asociación o empresa que, directa o indirectamente a través de uno o más intermediarios, controle, sea controlada por o esté bajo el control común de una parte, según corresponda, o sus respectivos sucesores. El término «control», incluidos los términos «controlar», «controlado por» y «bajo control común con», significa la posesión, directa o indirecta, del poder de dirigir o hacer que se dirija la gestión y las políticas de una sociedad, asociación o empresa, ya sea a través de la propiedad de acciones con derecho a voto, por contrato o de otro modo. Las filiales incluirán aquellas entidades que existan en la actualidad o que se establezcan posteriormente mediante inversión, fusión o de otro modo, incluidos los sucesores y cesionarios de dichas entidades.

1.2. **Leyes Aplicables**: todas y cada una de las leyes, reglamentos, decisiones impuestas por el gobierno, términos, directrices y cualquier modificación de los mismos, que tengan relevancia en la jurisdicción correspondiente, así como cualquier decisión tomada por entidades gubernamentales pertinentes y competentes, en todas las jurisdicciones pertinentes para el Contrato, incluyendo, entre otras, las normas que rigen la profesión de intermediación bancaria y cualquier código monetario y financiero aplicable en los países pertinentes, la legislación sobre la lucha contra el blanqueo de capitales (PBC), la financiación del terrorismo (FT), los embargos, las sanciones, el soborno, la conducta indebida, la información confidencial (incluida la propiedad intelectual y los secretos comerciales), el comportamiento de las instituciones financieras y las leyes de protección de datos.

1.3. **Responsable del tratamiento**: tiene el significado que se le da al término «responsable» cuando determina los fines de cualquier dato personal y los medios para su tratamiento, tal y como se establece en las leyes de protección de datos.

1.4. **Encargado del tratamiento**: tiene el significado que se le da al término «encargado» cuando cualquier otro organismo trata datos personales en nombre de un responsable del tratamiento, tal y como se establece en las leyes de protección de datos.

1.5. **Leyes de Protección de Datos**: el Reglamento General de Protección de Datos 2016/679 (RGPD), la nueva Ley Federal Suiza de Protección de Datos (nFADP), la Ley de Protección de Datos del Reino Unido de 2018, el Reglamento sobre Privacidad y Comunicaciones Electrónicas del Reino Unido de 2003, la Ley Francesa n.º 78-17, de 6 de enero de 1978, sobre tecnología de la información, archivos y libertades, y todas las demás leyes aplicables relacionadas con el tratamiento de datos personales, cada una de ellas con sus modificaciones, sustituciones o derogaciones correspondientes.

1.6. **Incidente de Seguridad de los Datos**: cualquier acceso, tratamiento, supresión, pérdida o cualquier forma de tratamiento ilícito de los datos personales (o los datos personales compartidos, según corresponda) no autorizados o accidentales, y/o cualquier brecha de la seguridad y/o la confidencialidad que dé lugar a la destrucción, pérdida, alteración, divulgación no autorizada o acceso accidental o ilícito a los datos personales (o los datos personales compartidos, según corresponda).

1.7. **Interesado**: persona física identificada o identificable a la que se refieren los Datos Personales.

1.8. **Solicitud del Interesado:** solicitud formal realizada por un interesado con el fin de ejercer sus derechos (i) a acceder a sus Datos Personales; (ii) a que se rectifiquen o supriman sus Datos Personales; (iii) a limitar u oponerse al tratamiento de sus Datos Personales; (iv) a solicitar la portabilidad de sus Datos Personales; (v) no ser objeto de decisiones automatizadas (incluida la elaboración de perfiles); o (vi) en relación con cualquier otro derecho que el interesado tenga derecho a ejercer en cualquier jurisdicción pertinente a la que se aplique el presente DPA.

1.9. **Datos Personales**: cualquier dato de carácter personal que identifique a una persona física (tal y como se establece en las Leyes de Protección de Datos) que se trate en relación con el Contrato.

1.10. **Datos Personales Compartidos**: cualquier dato personal que identifique a una persona física (tal y como se establece en las Leyes de Protección de Datos) que se trate en relación con el Contrato si las Partes actúan como Responsables independientes del tratamiento de datos en el contexto de una «relación entre Responsables del tratamiento de datos».

1.11. **Cláusulas contractuales tipo**: se refieren a (i) las cláusulas contractuales tipo para transferencias internacionales publicadas por la Comisión Europea el 4 de junio de 2021 que regulan la transferencia de datos personales desde el EEE a terceros países, tal y como han sido adoptadas por la Comisión Europea (disponibles en el sitio web de la Comisión Europea: Decisión de ejecución - 2021/914 - EN - EUR-Lex (europa.eu)), y el Comisionado Federal Suizo de Protección de Datos e Información (**«Swiss** FDPIC») en relación con las transferencias de datos a terceros países (en conjunto, **«SCC de la** UE»); (ii) el anexo sobre transferencias internacionales de datos («**Anexo de transferencias del Reino** Unido») adoptado por la Oficina del Comisionado de Información del Reino Unido («ICO del **Reino** Unido») para las transferencias de datos desde el Reino Unido a terceros países; (iii) cualquier cláusula similar (según corresponda) adoptada por un regulador de protección de datos en relación con las transferencias de datos a terceros países; o (iv) cualquier cláusula sucesora de (i) a (iii).

1.12. **Subencargado del tratamiento**: significa una entidad que un Encargado del tratamiento contrata para tratar datos personales en nombre de dicho Encargado del tratamiento.

1.13. **Autoridad de control**: significa una autoridad pública independiente que es: (i) establecida por un Estado miembro de la UE de conformidad con el artículo 51 del RGPD; o (ii) la autoridad pública que regula la protección de datos y que tiene autoridad de control y jurisdicción sobre usted.

2. Funciones de protección de datos

En el curso de la prestación de los Servicios por parte de Planet al Comerciante en virtud del Contrato, las Partes podrán, de vez en cuando, proporcionar o poner a disposición de la otra Parte Datos personales. Las Partes acuerdan que, en función de los Servicios contratados, las funciones de protección de datos que se les asignen a efectos de las Leyes de protección de datos serán: (i) Responsables del tratamiento independientes (en el contexto de una relación entre un Responsable del tratamiento y otro Responsable del tratamiento); (ii) Responsable del tratamiento de datos (en el contexto de una relación entre un Responsable del tratamiento y un Encargado del tratamiento); o (iii) Encargado del tratamiento en nombre de la otra Parte (en el contexto de una relación entre un Encargado del tratamiento y un Responsable del tratamiento). Teniendo esto en cuenta:

a) **Si las Partes tratan Datos Personales actuando como Responsables del Tratamiento independientes, se aplicará el párrafo 3 del presente DPA.**
b) **Si una Parte procesa Datos personales en calidad de Responsable del tratamiento, en el contexto de una relación entre un Responsable del tratamiento y un Encargado del tratamiento, se aplicará a dicha Parte el apartado 4 del presente DPA.**
c) **Si una Parte procesa Datos personales en calidad de Encargado del tratamiento, en nombre de la otra Parte, se aplicará a dicha Parte el párrafo 5 del presente DPA.**

En el Apéndice 1 se incluye una descripción completa de las funciones y los fines para los que se tratan los Datos personales (o los Datos personales compartidos, según corresponda) en el contexto de los servicios prestados en virtud del Contrato.

3. Obligaciones aplicables a las Partes que actúan como Responsables independientes del tratamiento

El presente apartado 3 se aplicará en caso de que las Partes actúen como Responsables independientes del tratamiento.

3.1. General

3.1.1. Las Partes se comunicarán periódicamente entre sí los Datos personales para los fines establecidos en el Contrato y/o el DPA (**«Datos Personales Compartidos**») y acuerdan que, en relación con dichos Datos personales compartidos, cada Parte actuará como Responsable del tratamiento por derecho propio y determinará de forma independiente los fines y los medios de dicho tratamiento de datos.

3.2. Tratamiento de los Datos personales compartidos

3.2.1. Cuando una Parte actúe como Responsable del tratamiento de los Datos Personales Compartidos en relación con los Servicios, será responsable de cumplir y cumplir con sus obligaciones en virtud de las Leyes de Protección de Datos y, en particular, de:

a) asegurarse de que los Datos Personales Compartidos proporcionados o puestos a disposición en virtud del Contrato sean precisos y estén actualizados;
b) garantizar que dispone de una base jurídica adecuada para el tratamiento de los Datos Personales Compartidos tal y como se describe en el presente DPA y/o en el Contrato;
c) asegurarse de que se faciliten todos los avisos e información sobre el tratamiento de datos correspondientes (comúnmente conocidos como «avisos de privacidad» o «políticas de privacidad») a los interesados afectados por el tratamiento de datos en el momento de recopilar sus datos personales, a fin de permitir el tratamiento lícito (incluida la recopilación y el intercambio) de los Datos Personales Compartidos para los fines establecidos en el Contrato y/o el DPA;
d) asegurarse de que, a menos que otra base jurídica establecida en las Leyes de Protección de Datos respalde la legitimidad del tratamiento, se obtenga y registre cualquier consentimiento necesario de los interesados para el tratamiento y, en caso de que un interesado revoque su consentimiento, garantizar que se comunique a la otra Parte.

3.2.2. Cada Parte se compromete a no proporcionar a la otra Parte ninguna categoría especial de Datos personales (como datos sobre la salud) que no sea necesaria para la prestación de los Servicios.

3.3. Seguridad de los datos

3.3.1. Cada Parte tomará las medidas razonables para garantizar la fiabilidad de las personas que puedan tratar los Datos Personales Compartidos, lo que incluye garantizar: (i) que el acceso se limite estrictamente a aquellas personas que necesiten conocer o acceder a los Datos personales compartidos pertinentes para los fines descritos en el Contrato y/o en el presente DPA; y (ii) que dichas personas estén sujetas a compromisos de confidencialidad u obligaciones profesionales o legales de confidencialidad.

3.3.2. Las Partes implementarán y mantendrán las medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad adecuado al riesgo (teniendo en cuenta la naturaleza, el alcance, el contexto y los fines del tratamiento), incluyendo el tratamiento no autorizado o ilícito, o la pérdida accidental, la destrucción o el daño de dichos Datos personales compartidos. En particular, Planet aplicará las siguientes medidas técnicas y organizativas que se encuentran en https://www.weareplanet.com/technical-and-organisational-measures, cuyo resumen se puede encontrar en el Apéndice 2.

3.3.3. La Parte que reciba los Datos Personales Compartidos no los conservará ni tratará durante más tiempo del necesario para los fines establecidos en el Contrato y/o en el presente DPA, y será responsable de aplicar las medidas adecuadas para garantizar que los Datos Personales Compartidos se destruyan o eliminen cuando no sean necesarios para dichos fines. No obstante lo anterior, cada Parte podrá seguir conservando los Datos Personales Compartidos de conformidad con los plazos de conservación legales o profesionales aplicables.

3.4. Derechos del Interesado

3.4.1. Cada Parte será responsable de gestionar sus propias Solicitudes de los Interesados en relación con los Datos personales compartidos y prestará la asistencia que sea razonablemente necesaria para que la otra Parte pueda cumplir con dichas Solicitudes de los Interesados.

3.4.2. Si una Parte recibe una Solicitud del interesado en relación con los Datos Personales Compartidos que se refieren al tratamiento respecto del cual la otra Parte es el Responsable del tratamiento, la Parte que reciba dicha Solicitud del Interesado la remitirá sin demora a la otra Parte. Previa solicitud razonable por escrito, la Parte que reciba la Solicitud del Interesado prestará la cooperación y asistencia razonables para que la otra Parte pueda cumplir con dicha Solicitud del Interesado y respetar los plazos aplicables establecidos en las Leyes de Protección de Datos.

3.5. Incidentes de seguridad de los datos

3.5.1. Cuando una Parte tenga conocimiento de un incidente de seguridad de los datos que tenga un impacto significativo en el tratamiento de los Datos Personales Compartidos, lo notificará sin demora a la otra Parte y cooperará con ella para que pueda investigar el incidente, formular una respuesta adecuada y tomar las medidas oportunas con respecto al incidente de seguridad de los datos.

3.5.2. En caso de que se produzca un incidente de seguridad de los datos relacionado con los Datos Personales Compartidos, o si se sospecha que se ha producido o puede producirse un incidente de seguridad de los datos, cada parte informará a la otra por escrito lo antes posible con toda la información pertinente sobre los detalles del incidente, a fin de que dicha parte pueda cumplir con las Leyes de Protección de Datos. La información pertinente sobre el incidente de seguridad de los datos incluirá:

a) nombre, nombre comercial e información que se alega que se ha visto afectada por él;
b) una descripción de su naturaleza, incluyendo, cuando sea posible, las categorías y el número aproximado de Interesados afectados;
c) el nombre y los datos de contacto del delegado de protección de datos u otro punto de contacto donde se pueda obtener más información;
d) una descripción de sus posibles consecuencias;
e) una descripción de las medidas adoptadas o propuestas para hacerle frente, incluidas, cuando proceda, las medidas para mitigar sus posibles efectos adversos; y
f) una copia de toda la correspondencia relacionada con ella, incluida cualquier correspondencia con los Interesados.

3.6. Asistencia mutua

3.6.1. Cada Parte, previa solicitud razonable, proporcionará a la otra Parte la asistencia, información y cooperación razonables para garantizar el cumplimiento de sus respectivas obligaciones en virtud de las Leyes de Protección de Datos.

3.6.2. Si una Parte recibe alguna queja, notificación o comunicación de una Autoridad Supervisora que se refiera directamente al tratamiento de Datos Personales Compartidos por la otra Parte, o a un posible incumplimiento por parte de dicha Parte de las Leyes de Protección de Datos en relación con los Servicios, la Parte que reciba la queja, notificación o comunicación deberá, en la medida en que lo permitan las Leyes Aplicables, notificarlo sin demora a la otra Parte y facilitarle la información que esta solicite razonablemente al respecto.

3.7. Transferencias Internacionales de Datos

3.7.1. Las Partes solo podrán tratar los Datos Personales Compartidos dentro del EEE, el Reino Unido o Suiza (según corresponda) o en otros países reconocidos por la Comisión Europea, la ICO o la FDPIC suiza (según corresponda), que garanticen un nivel adecuado de protección de los datos personales en lo que respecta a la privacidad de los datos y los derechos y libertades fundamentales de las personas.

3.7.2. Cuando una Parte transfiera o exporte Datos personales compartidos a un tercer país fuera del EEE, el Reino Unido o Suiza (según corresponda) sin un nivel adecuado de protección según lo declarado por la Comisión Europea, la ICO o la FDPIC suiza (según corresponda), deberá cumplir con sus obligaciones en virtud de las Leyes de protección de datos: (i) utilizando cualquier mecanismo de control de transferencias razonable reconocido por las Leyes de protección de datos como garantía adecuada; o (ii) regulando los términos de dicha transferencia mediante las cláusulas contractuales tipo, que se incorporarán al presente Contrato.

2.2. Además, la Parte que transfiera o exporte los Datos Personales Compartidos implementará e incorporará al presente DPA las medidas complementarias adecuadas que sean pertinentes de acuerdo con el riesgo normativo del país de destino, garantizando un nivel de protección de los datos esencialmente equivalente al del EEE, el Reino Unido o Suiza, según corresponda.

3.7.3. En la medida en que la Parte que transfiere o exporta los Datos Personales Compartidos se base en un mecanismo legal específico para normalizar las transferencias internacionales de datos y dicho mecanismo sea posteriormente modificado, revocado o declarado inválido por un tribunal de jurisdicción competente, las Partes acuerdan cooperar de buena fe para buscar un mecanismo alternativo adecuado que pueda respaldar legalmente la transferencia.

4. Obligaciones aplicables a una Parte que actúe como Responsable del Tratamiento

El presente apartado 4 se aplicará en caso de que una Parte actúe como Responsable del tratamiento en el contexto de una relación entre un Responsable del tratamiento y un Encargado del tratamiento.

4.1. General

4.1.1. Cuando una Parte actúe como Responsable del tratamiento y la otra Parte desempeñe la función de Encargado del tratamiento, la primera tendrá la autoridad única y exclusiva para determinar los fines y los medios del tratamiento de los Datos personales recibidos de la otra Parte o a través de ella, y será responsable de cumplir con sus obligaciones en virtud de las Leyes de protección de datos y, en particular, de:

a) asegurarse de que los Datos Personales facilitados o puestos a disposición en virtud del Contrato sean exactos y estén actualizados;
b) proporcionar únicamente instrucciones relacionadas con el tratamiento de datos personales que sean lícitas;
c) garantizar que dispone de una base jurídica adecuada para el tratamiento de los datos personales tal y como se describe en el presente DPA y/o en el Contrato;
d) asegurarse de que se faciliten todos los avisos de tratamiento justos necesarios (comúnmente conocidos como «avisos de privacidad» o «políticas de privacidad») a los interesados afectados por el tratamiento de datos en el momento de recopilar sus Datos Personales, a fin de permitir el tratamiento lícito (incluida la recopilación y el intercambio) de los Datos Personales para los fines establecidos en el Contrato y/o el DPA;
e) asegurarse de que, a menos que otra base jurídica establecida en las Leyes de Protección de Datos respalde la legalidad del tratamiento, se obtenga y registre el consentimiento necesario de los interesados para el tratamiento y, en caso de que un interesado revoque su consentimiento, asegurarse de que se comunique al Encargado del Tratamiento; y
f) aplicar y mantener las medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad adecuado al riesgo (teniendo en cuenta la naturaleza, el alcance, el contexto y los fines del tratamiento), incluido el tratamiento no autorizado o ilícito, o la pérdida accidental, la destrucción o el daño de dichos Datos Personales.

4.1.2. El Responsable del tratamiento se compromete a no proporcionar al Encargado del tratamiento ninguna categoría especial de datos personales (como datos sobre la salud) que no sea necesaria para la prestación de los servicios.

5. Obligaciones aplicables a una Parte que actúe como Encargado del Tratamiento

El presente apartado 5 se aplicará en caso de que una de las Partes actúe como Encargado del tratamiento en nombre de la otra Parte. A tal efecto, cuando una de las Partes trate Datos personales en nombre de la otra Parte, deberá cumplir con las obligaciones que le incumben en virtud de las Leyes de Protección de Datos aplicables en las jurisdicciones en las que opera, así como con las obligaciones asumidas en el presente DPA, tal y como se establece a continuación:

5.1. Seguridad de los datos

5.1.1. El Encargado del tratamiento:

a) cumplirá con las normas de seguridad de los datos comunicadas y/o acordadas con la otra Parte;
b) conservará todos los datos personales en un entorno seguro para garantizar que no se divulguen a terceros (salvo en los casos permitidos por el Contrato) ni sean objeto de uso indebido por parte de terceros;
c) tomará medidas razonables, teniendo en cuenta la naturaleza y los riesgos que presenta el tratamiento de datos, para garantizar que no se produzca ningún incidente de seguridad de los datos; y
d) no eludirá ninguna tecnología utilizada por nosotros u otros terceros para proteger el contenido accesible a través de los Servicios.

5.1.2. La Parte que actúe como Encargado del Tratamiento se compromete a aplicar todas las medidas técnicas y organizativas adecuadas para proteger los Datos Personales, teniendo en cuenta el estado de los conocimientos, los costes de aplicación y la naturaleza, el alcance, el contexto y los fines del tratamiento de datos, así como los riesgos, el grado de probabilidad y la gravedad para los derechos y libertades de los Interesados, con el fin de garantizar un nivel de seguridad adecuado al riesgo. En particular:

a) Cuando el Comerciante actúe como Encargado del Tratamiento, estará obligado a adoptar todas las medidas técnicas y organizativas adecuadas, incluidas, entre otras, las medidas establecidas en el Apéndice 3, para garantizar un nivel adecuado de seguridad de los Datos Personales (incluida su protección contra la destrucción, pérdida o alteración accidentales o ilícitas, y contra la divulgación o el acceso no autorizados).
b) Cuando Planet actúe como Encargado del tratamiento, aplicará las siguientes medidas técnicas y organizativas que se encuentran en https://www.weareplanet.com/technical-and-organisational-measures, cuyo resumen se puede encontrar en el Apéndice 2.

c) Sin limitar la naturaleza material de cualquier otra divulgación de Datos personales, el incumplimiento de este apartado 5.1 se considerará un incumplimiento material del Contrato.

5.2. Confidencialidad y secreto

5.2.1. El Encargado del tratamiento se compromete a mantener su deber de confidencialidad con respecto a los datos personales a los que haya tenido acceso como resultado del presente acuerdo. A tal fin, el encargado del tratamiento se asegurará de que las personas autorizadas para tratar los datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a obligaciones legales de confidencialidad, y de que todos sus respectivos empleados estén formados de acuerdo con sus respectivas responsabilidades en virtud de las leyes de protección de datos.

5.3. Instrucciones del Responsable del tratamiento

5.3.1. El Encargado del tratamiento tratará los Datos personales únicamente siguiendo las instrucciones escritas del Responsable del tratamiento (incluidas las documentadas en el presente DPA) en relación con los Servicios prestados en virtud del Contrato, y no podrá utilizarlos para ningún otro fin que no sea el especificado en el presente DPA y/o en el Contrato. El Encargado del tratamiento se compromete a informar al Responsable del tratamiento lo antes posible por escrito en caso de que considere que alguna de las instrucciones del Responsable del tratamiento pueda infringir las Leyes de Protección de Datos.

5.4. Subcontratación

5.4.1. El Encargado del tratamiento está autorizado a utilizar subencargados para llevar a cabo actividades que formen parte del presente Contrato. No obstante, si después de la fecha del presente Anexo el Encargado del tratamiento contrata a nuevos subencargados, el Responsable del Tratamiento podrá oponerse razonablemente al cambio o al uso de un nuevo subencargado por motivos legítimos, notificándolo por escrito al Encargado del tratamiento en un plazo de diez (10) días a partir de la notificación del nuevo subencargado. Si no se ha producido ninguna objeción, se considerará que el subencargado ha sido aceptado.

5.4.2. En particular, el Comerciante reconoce que los subencargados del tratamiento de Planet son esenciales para prestar los Servicios y que, si se opone al uso de un subencargado del tratamiento por parte de Planet, a pesar de cualquier disposición contraria en el Contrato (incluido el presente Anexo), Planet no estará obligada a prestar al Comerciante el Servicio para el que Planet utiliza dicho subencargado del tratamiento.

5.4.3. Los subencargados del tratamiento de Planet y del Comerciante se enumeran en el Apéndice 4 y, al firmar este Anexo, Planet y el Comerciante autorizan respectivamente a la otra Parte a utilizar dichos subencargados del tratamiento.

5.4.4. El Encargado del tratamiento celebrará un acuerdo por escrito con sus subencargados imponiendo obligaciones que sean coherentes con las del presente Anexo y/o el Contrato. Si un subencargado incumple sus obligaciones de protección de datos en virtud de dicho acuerdo, el Encargado del tratamiento estará obligado ante el Responsable del tratamiento por los actos y omisiones de su subencargado en la misma medida en que lo sería si prestara el Servicio correspondiente directamente en virtud del Contrato.

5.4.5. El Encargado del tratamiento acordará con el subencargado una cláusula de tercero beneficiario por la que, en caso de que el Encargado del tratamiento haya desaparecido de hecho, haya dejado de existir legalmente o se haya declarado insolvente, el Responsable del tratamiento tendrá derecho a rescindir el acuerdo con el subencargado y a ordenarle que borre o devuelva los datos personales.

5.5. Asistencia al Responsable del tratamiento, cumplimiento y auditorías

5.5.1. Mediante la aplicación de las medidas técnicas y organizativas adecuadas y en la medida de lo posible, el Encargado del tratamiento asistirá al Responsable del tratamiento en las Solicitudes de los Interesados que pueda recibir. El Responsable del tratamiento tendrá derecho a ordenar por escrito al Encargado del tratamiento que deje de responder a dichas solicitudes de los Interesados en cualquier momento. Cuando el Encargado del tratamiento reciba una Solicitud de un Interesado, responderá a dicha solicitud de conformidad con las Leyes de Protección de Datos aplicables. El Responsable del tratamiento reconoce que la gestión de dichas solicitudes de los interesados por parte del Encargado del tratamiento en nombre del Responsable del tratamiento no implica ninguna exención o renuncia a las obligaciones legales impuestas por las Leyes de Protección de Datos aplicables.

5.5.2. El Encargado del tratamiento, teniendo en cuenta la naturaleza del tratamiento y la información de que dispone, también ayudará al Responsable del tratamiento a garantizar el cumplimiento de las obligaciones derivadas de las leyes de protección de datos que sean pertinentes para el tratamiento de datos cubierto por el presente DPA, incluidas las

notificaciones a una autoridad de control o a los interesados, el proceso de realización de una evaluación de impacto sobre la protección de datos y las consultas previas con las autoridades de control.

5.5.3. El Encargado del Tratamiento pondrá a disposición del Responsable del Tratamiento toda la información necesaria para demostrar el cumplimiento de sus respectivas obligaciones establecidas en la presente Adenda y permitirá y contribuirá a las auditorías de datos, incluidas las inspecciones, si así lo requiere el Responsable del Tratamiento.

5.5.4. El Responsable del tratamiento podrá llevar a cabo, por cuenta propia, una vez al año, con un preaviso mínimo de 30 días, cualquier auditoría para confirmar el cumplimiento de las leyes de protección de datos. La auditoría será realizada por personal de cualquiera de las Partes o por una entidad independiente, elegida por la parte auditora, con miembros independientes que cuenten con las cualificaciones profesionales necesarias, sujetos a la obligación de confidencialidad y que no pertenezcan a una empresa que compita directamente con cualquiera de las Partes en relación con los Servicios. Las Partes acuerdan que:

a) la auditoría no incluirá datos financieros o personales que no estén directa y exclusivamente relacionados con cada una de las Partes, ninguna información que pueda afectar a los sistemas de seguridad y los datos de cada una de las Partes (es decir, riesgo para la confidencialidad de la información) y el código fuente de los programas informáticos utilizados en la prestación de los Servicios;
b) el auditor no copiará ningún documento, archivo, dato o información, en su totalidad o en parte, ni tomará fotografías, escaneará, realizará archivos o programas de audio/vídeo o informáticos sin consentimiento previo; y
c) la auditoría deberá realizarse durante el horario laboral y de manera que no perturbe las operaciones o los servicios de la Parte auditada.

5.6. Transferencias internacionales de datos

5.6.1. El Encargado del tratamiento podrá tratar Datos Personales dentro del EEE, el Reino Unido o Suiza (según corresponda) o en otros países reconocidos por la Comisión Europea, la ICO o la FDPIC suiza (según corresponda) como países que garantizan un nivel adecuado de protección de los Datos Personales en lo que respecta a la privacidad de los datos y los derechos y libertades fundamentales de los Interesados.

5.6.2. Cuando el Encargado del tratamiento transfiera o exporte datos personales a un tercer país fuera del EEE, el Reino Unido o Suiza (según corresponda) sin un nivel adecuado de protección según lo declarado por la Comisión Europea, la ICO o la FDPIC suiza (según corresponda), el Encargado del Tratamiento deberá cumplir con sus obligaciones en virtud de las Leyes de Protección de Datos: (i) utilizando cualquier mecanismo de control de transferencia razonable reconocido por las Leyes de Protección de Datos como garantía adecuada; o (ii) regulando los términos de esta transferencia mediante las Cláusulas Contractuales Tipo, que se incorporarán al presente DPA.

5.6.3. Además, el Encargado del tratamiento implementará e incorporará al presente DPA las medidas complementarias adecuadas que sean pertinentes de acuerdo con el riesgo normativo del país de destino, garantizando un nivel de protección de los datos esencialmente equivalente al del EEE, el Reino Unido o Suiza, según corresponda.

5.6.4. En la medida en que el Encargado del tratamiento se base en un mecanismo legal específico para normalizar las transferencias internacionales de datos y dicho mecanismo sea posteriormente modificado, revocado o declarado inválido por un tribunal de jurisdicción competente, las Partes acuerdan cooperar de buena fe para buscar un mecanismo alternativo adecuado que pueda respaldar legalmente la transferencia.

5.7. Incidentes de seguridad de los datos

5.7.1. Cuando el Encargado del tratamiento tenga conocimiento de un incidente de seguridad de los datos que tenga un impacto significativo en el tratamiento de los datos personales objeto del acuerdo, lo notificará sin demora al Responsable del tratamiento, cooperará en todo momento con este y seguirá sus instrucciones con respecto a dicho incidente de seguridad de los datos, con el fin de que el Responsable del tratamiento pueda llevar a cabo una investigación, formular una respuesta adecuada y adoptar las medidas adicionales oportunas al respecto.

5.7.2. En caso de que se produzca un incidente de seguridad de los datos, o si se sospecha que se ha producido o puede producirse un incidente de seguridad de los datos, el Encargado del tratamiento informará al Responsable del tratamiento por escrito lo antes posible con toda la información pertinente relativa a los detalles del incidente, con el

fin de ayudar al Responsable del tratamiento a cumplir con las leyes de protección de datos. La información pertinente del incidente de seguridad de los datos incluirá:

a) nombre, nombre comercial y la información que se alega que se ha visto afectada por él;
b) una descripción de su naturaleza, incluyendo, cuando sea posible, las categorías y el número aproximado de interesados afectados;
c) el nombre y los datos de contacto del delegado de protección de datos del Encargado del tratamiento u otro punto de contacto donde se pueda obtener más información;
d) una descripción de sus posibles consecuencias;
e) una descripción de las medidas adoptadas o propuestas por el Encargado del tratamiento para hacerle frente, incluidas, cuando proceda, las medidas para mitigar sus posibles efectos adversos; y
f) una copia de toda la correspondencia relacionada con el mismo, incluida cualquier correspondencia con los interesados.

5.8. Registro de actividades del tratamiento

5.8.1. El Encargado del tratamiento conservará un registro escrito de todas las categorías de actividades de tratamiento de datos realizadas en nombre del Responsable del tratamiento cuando actúe como Encargado del tratamiento, incluyendo:

a) el nombre y los datos de contacto del Responsable del tratamiento en cuyo nombre actúa, cualquier subencargado del tratamiento posterior y, en su caso, el delegado de protección de datos;
b) las categorías de actividades de tratamiento de datos realizadas en nombre del Responsable del tratamiento o del interesado;
c) cuando proceda, las transferencias de datos personales a un tercer país o a una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias a las que se refieren las leyes de protección de datos;
d) en la medida de lo posible, una descripción general de las medidas de seguridad técnicas y organizativas.

5.9. Devolución o destrucción de datos personales

5.9.1. Una vez prestado el Servicio contratado o tras la rescisión del Contrato, el Encargado del tratamiento devolverá y/o destruirá, a discreción del Responsable del tratamiento, y en la forma y en los plazos indicados por este, todos los Datos Personales a los que haya tenido acceso durante la relación contractual y cualquier otro documento considerado confidencial, salvo que alguna exigencia o impedimento legal requiera lo contrario.

5.9.2. No obstante lo anterior, si no se recibe dicha instrucción del Responsable del tratamiento en un plazo de 3 meses tras la prestación de los Servicios o la rescisión del Contrato, los Datos personales serán destruidos. El Responsable del tratamiento podrá solicitar al Encargado del tratamiento que le facilite un certificado escrito de destrucción de los Datos personales y los documentos destruidos.

5.9.3. Siempre que el Responsable del tratamiento acepte el presupuesto, el Encargado del tratamiento facilitará los Datos personales al Responsable del tratamiento o a cualquier tercero designado por este, en un formato estándar del mercado, con el fin de continuar con el tratamiento de los Datos personales.

6. Varios

6.1. El Anexo constituye el acuerdo completo entre Planet y el Comerciante en relación con su objeto y sustituye cualquier acuerdo anterior que las Partes pudieran haber tenido en relación con el mismo.

6.2. Salvo que se modifique o enmiende específicamente por los términos de este Anexo, el Contrato y todas las disposiciones contenidas en él o los términos de cualquier otro acuerdo o documento al que se haga referencia en él están y seguirán estando en pleno vigor y efecto.

6.3. En caso de que los términos de este Anexo entren en conflicto con los términos de cualquier otra enmienda o anexo y/o el Contrato en relación con el tratamiento de Datos Personales, prevalecerán los términos de este Anexo.

6.4. La ley aplicable y la jurisdicción con respecto a este Anexo serán las mismas que las establecidas en el Contrato.

EN FE DE LO CUAL, las partes han hecho que el presente Anexo sea debidamente firmado y entregado por sus representantes legítimos y debidamente autorizados en la fecha y el año indicados al principio del presente documento.

Planet	**Comerciante**
Por:_____	Por:_____
Nombre:	Nombre:
Cargo:	Título:

APÉNDICE 1

Finalidades del tratamiento

Las Partes entienden que Planet puede utilizar los Datos personales (o los Datos personales compartidos, según corresponda) en nombre del Interesado para:

a) Cumplir con sus obligaciones en virtud del Contrato (por ejemplo, permitir la gestión de transacciones);
b) Cumplir con sus obligaciones en virtud de las leyes aplicables y con los requisitos y solicitudes de las autoridades supervisoras (por ejemplo, verificar la identidad de los interesados);
c) Sus intereses legítimos (por ejemplo, mejorar nuestra retroalimentación sobre el compromiso con los servicios prestados);

Las Partes se comprometen a que los Datos Personales (o los Datos Personales Compartidos, según corresponda) nunca se venderán ni se facilitarán a terceros sin la autorización previa por escrito de los Interesados afectados.

Funciones en materia de protección de datos

Servicio	Planet	Comerciante	Categoría de datos y datos personales que se suelen tratar
Pasarela	Encargado del tratamiento	Responsable del tratamiento	Datos de los clientes del comerciante que utilizan los servicios, incluidos: PAN, CVV, fecha de caducidad y código postal cuando sea necesario para fines de verificación. Para APM, solo se procesa el número de cuenta.
Proxy PCI	Encargado del tratamiento	Responsable del tratamiento	Datos de los clientes del Comerciante que utilizan los Servicios, incluyendo: PAN, fecha de caducidad de la tarjeta, CVV.
Adquirencia	Responsable del tratamiento	Responsable del tratamiento	Datos del cliente del Comerciante que utiliza los Servicios, incluyendo: PAN, CVV, fecha de caducidad y código postal cuando sea necesario para fines de verificación. Para APM, solo se procesa el número de cuenta.
Alquiler de equipos	Encargado del tratamiento	Responsable del tratamiento	Ciertos datos limitados de los clientes del Comerciante que utilizan los Servicios relacionados con la transacción de pago realizada a través del equipo, incluyendo el importe de las transacciones y el código de autorización.
Compra de equipos	Encargado del tratamiento	Responsable del tratamiento	Ciertos datos limitados de los clientes del Comerciante que utilizan los Servicios relacionados con la transacción de pago realizada a través del equipo, incluyendo el importe de las transacciones y el código de autorización (si procede).
Conversión de divisas	Encargado del tratamiento	Responsable del tratamiento	Datos de los clientes del Comerciante que utilizan los Servicios, incluidos: dirección IP (solo para DCC), BIN de la tarjeta (primeros 6 dígitos), datos de la tarjeta tokenizada, información del dispositivo.
Reembolso del IVA	Responsable del tratamiento	Encargado del tratamiento	Datos de los clientes del comerciante que utilizan los Servicios: incluyendo PAN, CVV, fecha de caducidad y código postal cuando sea necesario para fines de verificación. Para APM, solo se procesa el número de cuenta.
Software de solución de tarjetas regalo	Responsable del tratamiento	Responsable del tratamiento	Datos de los clientes del Comerciante que utilizan los Servicios: nombre, dirección de correo electrónico y dirección postal (si se emite una tarjeta regalo física).
Software minorista	Encargado del tratamiento	Responsable del tratamiento	Datos de los clientes del Comerciante que utilizan los Servicios, incluyendo: nombre, dirección de correo electrónico, número de teléfono, dirección postal; información de inicio de sesión del usuario (dirección IP, tipo de navegador); información de facturación del usuario (información de contacto, últimos cuatro dígitos de la tarjeta de crédito y tipo de método de pago).

APÉNDICE 2

Cuando Planet procese Datos Personales (o Datos Personales Compartidos, según corresponda), aplicará las siguientes Medidas técnicas y organizativas que se encuentran en https://www.weareplanet.com/technical-and-organisational-measures, cuyo resumen se incluye a continuación:

Categoría	Subcategoría	Medida
Programas y políticas de seguridad	Programa de seguridad	Planet mantiene y aplica un programa de seguridad que rige la forma en que Planet gestiona la seguridad.
	Programa de privacidad	Planet mantiene y aplica un programa de privacidad que rige la forma en que se recopilan, utilizan y comparten los datos personales.
Gestión de riesgos y activos	Evaluaciones de riesgos	Planet gestiona los riesgos de forma proactiva a través de nuestro Marco de Gestión de Riesgos Empresariales y nuestro sólido Modelo de Tres Líneas.
	Gestión de activos	Planet mantiene y aplica un programa de gestión de activos que clasifica y controla adecuadamente los activos de hardware y software a lo largo de su ciclo de vida.
Formación y controles del personal	Reconocimiento de responsabilidad	Todos los empleados de Planet y los contratistas independientes que puedan tener acceso a datos, incluidos aquellos que procesan datos personales, reconocen sus responsabilidades en materia de seguridad y privacidad de los datos en virtud de las políticas de Planet.
Formación y concienciación	Formación anual sobre seguridad y privacidad	Los empleados de Planet completan una formación anual de sensibilización sobre el RGPD, KYC, AML y seguridad de la información.
Gestión de redes y operaciones	Políticas y procedimientos	Planet implementa políticas y procedimientos para la gestión de redes y operaciones. Estas políticas y procedimientos abordan el refuerzo de la seguridad, el control de cambios, la segregación de funciones, la separación de los entornos de desarrollo y producción, la gestión de la arquitectura técnica, la seguridad de la red, la protección contra malware, la protección de los datos en tránsito y en reposo, la integridad de los datos, el cifrado, los registros de auditoría y la segregación de la red.
	Evaluaciones de vulnerabilidad	Planet realiza evaluaciones periódicas de vulnerabilidad y pruebas de penetración en sus sistemas y aplicaciones, incluidos aquellos que procesan datos personales.
Controles de acceso técnico	Control de acceso	Planet implementa medidas para evitar que personas no autorizadas utilicen los sistemas de procesamiento de datos.
	Control de acceso a los datos	Planet implementa medidas para garantizar que las personas con derecho a utilizar un sistema de procesamiento de datos solo tengan acceso a los datos personales permitidos por sus derechos de acceso, y que los datos personales no puedan ser leídos, copiados, modificados o eliminados sin autorización.
Controles de acceso físico	Seguridad del centro de datos	Planet recurre a proveedores de servicios externos de confianza para alojar su infraestructura de producción. Planet depende de estos terceros para supervisar los controles de acceso físico a las instalaciones del centro de datos bajo su gestión.
	Seguridad de las oficinas	El acceso físico a las oficinas de Planet se controla mediante mecanismos como el registro de visitantes, cerraduras electrónicas, sistemas de alarma y salas de almacenamiento seguras.
	Auditorías de terceros	Planet revisa los informes de auditoría de terceros para verificar que los proveedores de servicios de Planet mantienen los controles de acceso físico adecuados para nuestros centros de datos gestionados.

Categoría	Subcategoría	Medida
Controles de disponibilidad	Disponibilidad	Planet ha implementado medidas para garantizar la rápida restauración de la disponibilidad y el acceso a los datos personales en caso de incidente físico o técnico.
Controles de divulgación	Divulgación	Planet implementa medidas para garantizar que los datos personales no puedan ser leídos, copiados, modificados o eliminados sin autorización durante la transmisión electrónica, el transporte o el almacenamiento en soportes (manuales o electrónicos).
Controles de separación	Separación	Planet implementa medidas para garantizar que los datos personales recopilados para diferentes fines puedan procesarse por separado.
Certificaciones	Cumplimiento de la normativa PCI	Planet se compromete a prestar sus servicios de conformidad con las normas de cumplimiento PCI-DSS, según sean aplicables a nuestras ofertas.
Cifrado	Mecanismos de cifrado	Planet emplea mecanismos de cifrado de datos en diversas etapas para reducir el riesgo de acceso no autorizado a los datos tanto en reposo como en tránsito. Además, el acceso a los materiales de claves criptográficas de Planet está limitado a un grupo selecto de personal autorizado de Planet.
Gestión y notificación de incidentes de seguridad de datos	Gestión de incidentes	Planet implementa un programa de gestión de incidentes de seguridad de datos que rige la forma en que Planet gestiona los incidentes.
Retención y eliminación de datos	Retención de datos	Planet implementa y mantiene políticas y procedimientos de retención de datos relacionados con los datos personales y revisa estas políticas y procedimientos según corresponda.

APÉNDICE 3

Cuando Planet actúa como Responsable del tratamiento de datos y el Comerciante como Encargado del tratamiento, el Comerciante está obligado a aplicar las siguientes medidas técnicas y organizativas para garantizar un nivel de seguridad acorde con el riesgo, incluyendo, entre otras, según corresponda:

1. Establecer las funciones y responsabilidades del personal que trata los datos personales e informar al personal de sus funciones y responsabilidades en lo que respecta al cumplimiento de las leyes y reglamentos de protección de datos.
2. Definir las funciones y perfiles de los usuarios de las aplicaciones y sistemas a través de los cuales se tratan los datos personales, de acuerdo con las funciones y responsabilidades establecidas, con el fin de evitar cualquier acceso no autorizado a los datos personales o a los recursos. Este sistema de control de acceso debe garantizar mecanismos adecuados de identificación y autenticación de los usuarios, tales como contraseñas que deben restablecerse periódicamente, datos biométricos, autenticación multifactorial, bloqueo automático del usuario tras un número determinado de intentos fallidos de inicio de sesión;
3. Aplicar medidas que permitan la seudonimización y el cifrado de los datos personales.
4. Poner en práctica registros de control y acceso a los archivos y soportes que contengan datos personales, que también deben contar con mecanismos para restringir el acceso.
5. Aplicar medidas automatizadas que restrinjan ese acceso a los usuarios no autorizados o cuando haya expirado el período de almacenamiento pertinente, como técnicas de borrado y seudonimización de datos.
6. Implementar procedimientos para limitar el acceso físico a las instalaciones en las que se encuentran los sistemas de información o los soportes físicos.
7. Aplicar medidas para garantizar la confidencialidad, integridad, disponibilidad y resiliencia continuas de los sistemas y servicios.
8. Implementar procedimientos para recuperar los datos personales si se destruyen, pierden o alteran, bajo la supervisión y con la aprobación del delegado de protección de datos.
9. Implementar procedimientos para detectar, evaluar y, si es necesario, notificar cualquier incidente de seguridad de los datos que pueda afectar a los derechos y libertades de los interesados.
10. Realizar revisiones periódicas del cumplimiento y definir y ejecutar planes de acción para mitigar los riesgos detectados;
11. Aplicar cualquier otra medida técnica y organizativa adecuada para garantizar un nivel de seguridad acorde con el riesgo.

ANEXO 4

Los subencargados del tratamiento de Planet pueden consultarse en: https://www.weareplanet.com/legal/subprocessor-and-service-provider-list

Los subencargados del tratamiento del comerciante son los siguientes: