

La presente Adenda de Tratamiento de Datos y sus Anexos ("**DPA**" del inglés *Data Processing Addendum*, o "**Adenda**") se formaliza entre usted (el **Ciente**) y nosotros (**Soprano**), y entra en vigor después de que el Cliente acepte el Contrato, únicamente en la medida en que la Legislación sobre Protección de Datos resulte de aplicación al tratamiento de los Datos Personales del Cliente por parte de Soprano en lo que a la prestación de los Servicios se refiere.

El Cliente formaliza este DPA en su propio nombre, incluyendo cuando proceda las Cláusulas Contractuales Tipo, y en nombre de las Filiales Autorizadas del Cliente (tal y como se define más adelante) en la medida en que el presente DPA y la Legislación sobre Protección de Datos lo exijan. El Cliente declara y garantiza que está autorizado para consentir y suscribir este DPA, incluyendo cuando corresponda las Cláusulas Contractuales Tipo, en nombre de cada Filial Autorizada del Cliente.

Podemos actualizar las condiciones del DPA cuando sea oportuno conforme a lo dispuesto en el apartado 1.3 de nuestras Condiciones de Servicio.

Los términos empleados en la presente Adenda tendrán el significado que se establece en la misma. Los términos en mayúsculas que no se definen de otra forma en esta Adenda tendrán el significado que se les atribuye en el Contrato. Salvo lo modificado expresamente a continuación, las condiciones del Contrato seguirán plenamente vigentes.

Considerando las obligaciones mutuas establecidas en la presente Adenda, las partes convienen en que los términos y condiciones dispuestos a continuación se incorporarán al Contrato a modo de Adenda. Salvo en caso de que el contexto requiera lo contrario, las referencias al Contrato mencionadas en esta Adenda se entenderán como referidas al Contrato en su versión modificada por esta Adenda, e incluyendo esta última.

1. Definiciones

- 1.1 En la presente Adenda, los siguientes términos tendrán los significados que se establecen a continuación y los términos análogos se interpretarán en consonancia:
 - 1.1.1 "**Contrato**" hace referencia a los documentos enumerados en el apartado 1.1 de las Condiciones de Servicio de Soprano o a otro acuerdo por escrito o en formato electrónico celebrado entre Soprano y el Cliente para la prestación de los Servicios.
 - 1.1.2 "**Encargado del Tratamiento Contratado**" o "**Encargado Contratado**" es Soprano o un Subencargado del tratamiento.
 - 1.1.3 "**Ciente**" significa la entidad jurídica del Cliente descrita en el Formulario de Solicitud que ha solicitado recibir nuestros Servicios.
 - 1.1.4 "**Filial del Cliente**" significa cualquier entidad que sea titular de o controle, o bien pertenezca a o esté controlada por, o se encuentre sujeta a un

mismo control o titularidad junto con el Cliente; entendiéndose por control la posesión directa o indirecta de la facultad para dirigir o hacer dirigir la gestión y las políticas de una entidad, ya sea por ostentar la propiedad de títulos con derecho de voto, en virtud de un contrato o de otro modo.

- 1.1.5 **"Filial Autorizada del Cliente"** significa (i) el Cliente y (ii) cualquier Filial del Cliente a la que Soprano le haya permitido hacer uso de los Servicios con arreglo al Contrato, aunque no haya presentado un Formulario de Solicitud (únicamente en la medida en que Soprano trate Datos Personales del Cliente).
- 1.1.6 **"Datos Personales del Cliente"** significa cualesquiera Datos Personales remitidos por o en nombre del Cliente mediante el uso de los Servicios, y tratados por el Encargado Contratado en representación de una Filial Autorizada del Cliente en relación o de conformidad con el Contrato.
- 1.1.7 **"Legislación sobre Protección de Datos"** hace referencia a todas las leyes y reglamentos aplicables en materia de privacidad, incluyendo, entre otros, la Legislación sobre Protección de Datos de la UE, Legislación sobre Protección de Datos de UK, y la legislación sobre protección de datos de Australia, Reino Unido, Singapur, Filipinas, Nueva Zelanda, Colombia, Brasil y Estados Unidos, en tanto en cuanto resulte de aplicación al Tratamiento de los Datos personales del cliente en virtud del Contrato.
- 1.1.8 **"EEE"** se entiende como el Espacio Económico Europeo.
- 1.1.9 **"Legislación sobre Protección de Datos de la UE"** hace referencia a toda la normativa en materia de protección de datos aplicable en la Unión Europea y en el Espacio Económico Europeo, incluyendo el RGPD y las transposiciones nacionales pertinentes de cada Estado miembro, en su versión oportunamente modificada o reemplazada, incluso por el RGPD y la legislación que lo complementa o lo ejecuta.
- 1.1.10 **"Cláusulas Tipo R-a-E de la UE"** significa las Cláusulas Contractuales Tipo, secciones I, II, III y IV (según corresponda) en la medida en que hagan referencia al Módulo Dos (Responsable a Encargado).
- 1.1.11 **"Cláusulas Tipo E-a-E de la UE"** significa las Cláusulas Contractuales Tipo, secciones I, II, III y IV (según corresponda) en la medida en que hagan referencia al Módulo Tres (Encargado a Encargado).
- 1.1.12 **"RGPD"** o **"UE RGPD"** es el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- 1.1.13 **"Legislación"** son las leyes, decretos, reglamentos, estatutos, normas obligatorias o códigos del sector, incluidas las exigencias e indicaciones de cualquier autoridad pública o legal competente aplicables a los Servicios o que afecten de otro modo a los Datos Personales del Cliente.

1.1.14 **"Datos Personales"** es cualquier información relativa a una persona física identificada o identificable ("el Interesado"), cuando y en la medida en que dicha información esté amparada por la Legislación sobre Protección de Datos aplicable.

1.1.15 **"Transferencia Restringida"** significa:

1.1.15.1 una transferencia de Datos Personales del Cliente desde cualquier Filial Autorizada del Cliente a un Encargado Contratado ubicado en un país fuera del EEE (cuando el UE RGPD sea de aplicación o los Datos Personales se exporten desde el EEE) o fuera de UK (cuando el UK RGPD resulte de aplicación o los Datos personales se exporten desde UK);

1.1.15.2 o una transferencia ulterior de los Datos Personales del Cliente desde un Encargado Contratado a otro Encargado Contratado ubicado en un país fuera del EEE (cuando los Datos Personales se exporten desde el EEE) o fuera de UK (cuando los Datos personales se exporten desde UK), o entre dos establecimientos de un Encargado Contratado,

en todos los casos, cuando dicha transferencia estuviera prohibida por la Legislación sobre Protección de Datos (o por las condiciones de los contratos de transferencia de datos establecidos para abordar las restricciones en transferencias de datos de la Legislación sobre Protección de Datos) en ausencia de las garantías adecuadas en virtud del apartado 5.4.1 o la cláusula 11 del presente.

1.1.16 **"Servicios"** se entiende como los servicios y otras actividades a prestar o desempeñar por o en nombre de Soprano a las Filiales Autorizadas del Cliente con arreglo al Contrato.

1.1.17 **"Soprano"** es la entidad Soprano descrita en el Formulario de Solicitud.

1.1.18 **"Filial de Soprano"** significa cualquier entidad que sea titular de o controle, o bien pertenezca a o esté controlada por, o se encuentre sujeta a un mismo control o titularidad junto con Soprano; entendiéndose por control la posesión directa o indirecta de la facultad para dirigir o hacer dirigir la gestión y las políticas de una entidad, ya sea por ostentar la propiedad de títulos con derecho de voto, en virtud de un contrato o de otro modo.

1.1.19 **"Cláusulas Contractuales Tipo"** o **"CCTs"** son:

- i. En el caso de Datos Personales exportados desde el EEE, las cláusulas contractuales tipo adoptadas por la decisión 2021/914 el 4 de junio de 2021 para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, según lo establecido en https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj ("UE CCTs")

- ii. En el caso de datos personales exportados desde el Reino Unido, la Adenda de transferencia internacional a las cláusulas contractuales tipo de la UE según se establece en <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/> ("UK CCTs")

en cada caso, según puedan modificar, completar o sustituir de vez en cuando las autoridades competentes.

- 1.1.20 **"Subencargado del tratamiento"** es cualquier persona física o jurídica (incluyendo cualquier tercero y cualquier Filial de Soprano, pero excluyendo a cualesquiera empleados de Soprano) nombrada por o en nombre de Soprano o su subencargado para tratar los Datos Personales en nombre de cualquier Filial Autorizada del Cliente en relación con la prestación de Servicios al Cliente.
- 1.1.21 **"Legislación sobre Protección de Datos de UK"** es Data Protection Act 2018 (UK) (que incorpora el UK RGPD) y la Privacy and Electronic Communications (EC Directive) Regulations 2003 y las leyes que la implementan o complementan;
- 1.1.22 **"UK RGPD"** significa la UK General Data Protection Regulation tal como se define en el Data Protection Act 2018 (UK).
- 1.1.23 **"UK"** significa el Reino Unido.
- 1.2 Los términos **"Comisión"**, **"Responsable del Tratamiento"** o **"Responsable"**, **"Interesado"**, **"Estado Miembro"**, **"Violación de la Seguridad de los Datos Personales"**, **"Tratamiento"**, **"Encargado del Tratamiento"** o **"Encargado"** y **"Autoridad de Control"** revisten el mismo significado que en el RGPD o UK RGPD (según corresponda), y sus términos análogos se interpretarán en consonancia.
- 1.3 Las referencias genéricas en este Anexo a "RGPD" Tendrán el mismo significado que la referencia equivalente en la Legislación sobre Protección de Datos de UK en relación con los Datos Personales originados en UK o sujetos a la Legislación sobre Protección de Datos de UK.
- 1.4 La palabra **"incluir"** se interpretará de tal modo que signifique 'incluir sin limitación alguna', y los términos análogos se interpretarán en consonancia.

2. Tratamiento de los Datos Personales del Cliente

2.1 Soprano se compromete a:

- 2.1.1 cumplir toda Legislación sobre Protección de Datos aplicable al Tratamiento de los Datos Personales del Cliente;

2.1.2 y tratar los Datos Personales del Cliente únicamente siguiendo las instrucciones documentadas del Cliente, salvo que el Tratamiento esté exigido por la Legislación aplicable a la que el Encargado contratado esté sujeto, en cuyo caso, en tanto en cuanto la Legislación lo permita, Soprano informará de dicho requisito legal a la Filial Autorizada del Cliente en cuestión, antes de llevar a cabo dicho Tratamiento de Datos Personales.

2.2 Cada Filial Autorizada del Cliente:

2.2.1 Ordena a Soprano (y proporciona la autorización general a Soprano para indicar a cada Subencargado) que:

2.2.1.1 Trate los Datos Personales del Cliente en nombre de cada Filial Autorizada del Cliente en función de las instrucciones del Cliente que se establecen en el Contrato y en la presente Adenda; y

2.2.1.2 En particular, transfiera los Datos Personales del Cliente a cualquier país o territorio,

según sea necesario para la prestación de los Servicios y con arreglo al Contrato.

2.2.2 Acepta que cualquier instrucción de una Filial Autorizada del Cliente será comunicada a Soprano exclusivamente por el Cliente y de forma escrita, tal y como se recoge en el Contrato, y el Cliente declara y garantiza que está y estará debida y correctamente autorizado en todo momento para dar las instrucciones establecidas en el apartado 2.2.1 en nombre de cada Filial Autorizada del Cliente.

2.2.3 Será el único responsable de:

2.2.3.1 velar por la exactitud, calidad y licitud de los Datos Personales del Cliente y los medios por los que se obtienen dichos Datos,

2.2.3.2 y cumplir con cualesquiera principios en materia de protección de datos contemplados en la Legislación sobre Protección de Datos en lo que respecta a la recogida y tratamiento de los Datos Personales del Cliente.

2.2.4 Deberá asegurarse de que sus instrucciones cumplan con toda la Legislación aplicable, incluyendo la Legislación sobre Protección de Datos.

2.2.5 Garantiza que tiene derecho a transferir o facilitar el acceso a Soprano a los Datos Personales del Cliente según se establece en la presente Adenda. Cada Filial Autorizada del Cliente será responsable de informar a los Interesados pertinentes sobre el Tratamiento de sus Datos Personales a los efectos de la Legislación sobre Protección de Datos vigente, en particular sobre el uso por parte de los Encargados Contratados para tratar sus Datos Personales y de que sus Datos Personales pueden ser objeto de una Transferencia Restringida.

- 2.3 El Anexo 1 de la presente Adenda recoge cierta información con respecto al Tratamiento de los Datos Personales del Cliente por parte de los Encargados Contratados según lo requiere el Artículo 28(3) del RGPD (y, posiblemente, los requisitos equivalentes de otra Legislación sobre Protección de Datos) incluyendo el objeto, la duración, la naturaleza y la finalidad del tratamiento, los tipos de Datos Personales del Cliente y las categorías de interesados. El Cliente puede, cuando lo considere oportuno, realizar modificaciones justificadas al Anexo 1 mediante notificación por escrito a Soprano en tanto en cuanto el Cliente considere necesario cumplir tales requisitos.
- 2.4 Soprano y cada Filial Autorizada del Cliente reconocen y aceptan que, en lo que al tratamiento de los Datos Personales del Cliente se refiere, una Filial Autorizada del Cliente podrá, según el caso, actuar en calidad de Responsable o Encargado del Tratamiento (incluyendo, sin limitación alguna, un Encargado en el sentido del Artículo 28(4) del RGPD) de los Datos Personales del Cliente. Soprano actuará en nombre de la Filial Autorizada del Cliente en calidad de Encargado del Tratamiento (incluyendo, sin carácter exhaustivo, un Encargado con el significado que se recoge en el Artículo 28(4) del RGPD).
- 2.5 Cuando una Filial Autorizada del Cliente tenga la condición de Encargado del Tratamiento (incluyendo, sin limitación alguna, un Encargado en el sentido del Artículo 28(4) del RGPD) que actúa en nombre de un Responsable, además de cumplir el apartado 2.2, el Cliente, en nombre de la Filial Autorizada del Cliente:
- 2.5.1 declara y garantiza que está y estará debida y correctamente autorizado en todo momento por el Responsable del Tratamiento para acordar y suscribir el presente DPA en nombre de dicho Responsable.
 - 2.5.2 se asegurará de que sus indicaciones se ajusten a las instrucciones directas del Responsable del Tratamiento, además de cumplir toda la Legislación aplicable, incluyendo la Legislación sobre Protección de Datos. Soprano únicamente tratará los Datos Personales del Cliente siguiendo instrucciones directas documentadas del Cliente de conformidad con el apartado 2.2.2. Soprano no recibirá instrucciones directas del Responsable salvo que Soprano y el Cliente lo hayan acordado por escrito.
 - 2.5.3 declara y garantiza que tiene derecho a transferir, facilitar el acceso o permitir el Tratamiento de los Datos Personales del Cliente a/por parte de los Encargados Contratados según se recoge en la presente Adenda. Por lo tanto, la Filial Autorizada del Cliente informará al Responsable del Tratamiento sobre el uso por parte de los Encargados Contratados para tratar los Datos Personales del Cliente, así como de que los Datos Personales del Cliente pueden ser objeto de una Transferencia Restringida.

3. Personal de Soprano

Soprano adoptará medidas razonables para garantizar que todo empleado, representante o contratista de cualquier Encargado Contratado que esté autorizado para tratar los Datos Personales del Cliente con arreglo al Contrato, o con el fin de cumplir la Legislación aplicable en el marco de las responsabilidades individuales del Encargado Contratado, está sujeto a los compromisos de confidencialidad o a las obligaciones profesionales o legales de confidencialidad.

4. Seguridad

- 4.1 Teniendo en cuenta el estado de la técnica, el coste de su aplicación y la naturaleza, el alcance, el contexto y las finalidades del Tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y las libertades de las personas físicas, Soprano, en lo tocante a los Datos Personales del Cliente, se compromete a aplicar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, incluyendo, cuando corresponda, las medidas a las que se hace referencia en el Artículo 32(1) del RGPD.

5. Subtratamiento

- 5.1 Cada Filial Autorizada del Cliente otorga una autorización general a Soprano para nombrar Subencargados y autoriza a cada Subencargado designado conforme a la presente cláusula 5, a nombrar a cualesquiera otros Subencargados de acuerdo con la presente cláusula 5 y el Contrato.
- 5.2 Soprano y cada Filial de Soprano que actúe en calidad de Subencargado puede seguir valiéndose de los Subencargados ya contratados a la fecha de esta Adenda, a reserva de que Soprano y el Subencargado cumplan en cada caso tan pronto como sea posible las obligaciones indicadas en el apartado 5.4.1.
- 5.3 Soprano conviene en mantener y poner a disposición del Cliente un listado actualizado de sus Subencargados y respectivas ubicaciones a petición escrita de este. Al menos 10 días antes de autorizar a cualquier nuevo Subencargado para que trate los Datos Personales del Cliente, Soprano notificará al Cliente cualquier cambio previsto en relación con la incorporación o sustitución de dicho Subencargado, actualizando el listado para este fin según corresponda. El Cliente puede suscribirse para recibir notificaciones por correo electrónico con las actualizaciones del listado de Subencargados de Soprano utilizando la información de contacto facilitada en el Anexo 1. Si el Cliente se suscribe, Soprano le notificará, con al menos 10 días de antelación, cualquier cambio previsto que afecte al Cliente en relación con la incorporación o sustitución de dicho Subencargado, ofreciéndole la oportunidad de oponerse a tales modificaciones dentro de ese plazo. Soprano informará al Cliente en caso de que no pueda satisfacer de manera razonable la oposición de este. El Cliente puede, mediante notificación por escrito a Soprano en el plazo de 30 días desde la notificación de este último, resolver el Contrato en la medida en que la resolución se refiera a los Servicios que requieran el uso del nuevo Subencargado objetado.
- 5.4 Soprano, con respecto a cada Subencargado:
 - 5.4.1 garantizará que el acuerdo entre Soprano y el Subencargado, o entre un Subencargado y otro Subencargado (de éste), se rige por un contrato por escrito que incluya condiciones que ofrezcan, al menos sustancialmente, el mismo nivel de protección para los Datos Personales del Cliente que el establecido en la presente Adenda, y que cumpla los requisitos del Artículo 28(3) del RGPD, con la salvedad del apartado 9.3 de este DPA;

- 5.4.2 solicitará el listado de Subencargados a sus Subencargados (los de Soprano) a petición por escrito del Cliente, en la medida en que sea razonablemente posible.
- 5.5 En cualquier caso, Soprano sigue siendo responsable ante el Cliente del cumplimiento de las obligaciones en materia de protección de datos, en virtud de la presente Adenda, por parte de cualquier Subencargado si este último no cumpliera sus obligaciones de protección de datos tal y como se describen en la presente cláusula 5.
- 5.6 Cada Filial Autorizada del Cliente declara y garantiza que está y estará debida y correctamente autorizada en todo momento por el Responsable pertinente para subcontratar el Tratamiento de los Datos Personales del Cliente a Soprano cuando dicha Filial esté capacitada para actuar en calidad de Encargado del Tratamiento de los Datos Personales del Cliente.

6. Derechos de los Interesados

- 6.1 Considerando la naturaleza del Tratamiento, Soprano asistirá a cada Filial Autorizada del Cliente, mediante la implementación de las medidas técnicas y organizativas adecuadas, en tanto en cuanto resulte posible, cumpliendo las obligaciones de las Filiales Autorizadas del Cliente, para responder a las peticiones de ejercicio de los derechos de los Interesados en virtud de la Legislación sobre Protección de Datos. Dichas peticiones de asistencia por parte de las Filiales Autorizadas del Cliente, serán comunicadas a Soprano exclusivamente por el Cliente de forma escrita, y Soprano solo tendrá obligación de responder directamente al Cliente. En aras de la claridad, las Filiales Autorizadas del Cliente son responsables de responder a dichas peticiones.
- 6.2 Soprano se comprometerá a:
 - 6.2.1 notificar al Cliente si un Encargado del Tratamiento Contratado recibe una petición de un Interesado con arreglo a cualquier Legislación sobre Protección Datos, respecto de los Datos Personales del Cliente, y a redirigir al Interesado para que presente su petición directamente al Cliente; y
 - 6.2.2 garantizar que el Encargado del Tratamiento Contratado no responda a dicha petición salvo siguiendo instrucciones documentadas del Cliente o de la Filial del Cliente que corresponda, en la medida en que el Cliente no pueda acceder a la información ni a los Datos Personales pertinentes tras hacer todo lo que esté razonablemente a su alcance, o según lo requiera la Legislación vigente a la que esté sujeto el Encargado Contratado.

7. Violación de la Seguridad de los Datos Personales

- 7.1 Soprano informará al Cliente sin dilación indebida en caso de que se percate de una Violación de la Seguridad de los Datos Personales que afecte a los Datos Personales del Cliente, proporcionado a este último la información disponible para asistir a la Filial Autorizada del Cliente en sus obligaciones de notificar dicha Violación a las Autoridades de Control o comunicarla a los Interesados en virtud de la Legislación sobre Protección De datos. Soprano facilitará dicha información

exclusivamente al Cliente, quien deberá informar a las Filiales Autorizadas del Cliente como corresponde y sin demora injustificada.

- 7.2 La notificación de, o la respuesta a una Violación de la Seguridad de los Datos Personales en virtud de la presente Adenda por parte de Soprano o de cualquier otro Encargado Contratado no se interpretará como un reconocimiento por su parte de ningún incumplimiento o responsabilidad con respecto a dicha Violación. El Cliente debe notificar inmediatamente a Soprano cualquier posible uso indebido de sus cuentas o credenciales de autenticación o de las de las Filiales Autorizadas del Cliente, así como cualquier Violación de Seguridad de los Datos Personales u otra incidencia de seguridad relacionada con los Servicios.
- 7.3 Por cuenta exclusiva del Cliente y en la medida en que no pueda acceder a la información necesaria para cumplir sus obligaciones en virtud de la Legislación sobre Protección de Datos aplicable, Soprano cooperará con el Cliente y con cada Filial Autorizada del Cliente y tomará tantas medidas comerciales razonables como le indique el Cliente para ayudar en la investigación, mitigación y reparación de dicha Violación.
- 7.4 El Cliente es el único responsable de cumplir con las obligaciones de notificación a cualquier tercero relativas a una Violación de la Seguridad de los Datos Personales, salvo cuando la Legislación sobre Protección de Datos disponga lo contrario.

8. Evaluación de impacto en la protección de datos y consulta previa

Soprano proporcionará asistencia razonable a cada Filial Autorizada del Cliente con cualesquiera evaluaciones de impacto relativas a la protección de datos, y previa consulta con las Autoridades de Control u otras autoridades competentes en materia de privacidad de datos, que el Cliente razonablemente considere adecuado exigir a cualquier Filial Autorizada del Cliente en virtud del Artículo 35 o 36 del RGPD o de las disposiciones equivalentes de cualquier otra Legislación sobre Protección de Datos, en todo caso únicamente en relación con el Tratamiento de los Datos Personales del Cliente por parte de los Encargados Contratados y teniendo en cuenta la naturaleza del Tratamiento y la información a disposición de estos.

9. Supresión o devolución de los Datos Personales del Cliente

- 9.1 Con sujeción al apartado 9.2, Soprano suprimirá o devolverá, sin demora, los Datos Personales del Cliente a la Filial Autorizada del Cliente (si los Datos Personales del Cliente no se han facilitado previamente ni se han puesto a disposición del Cliente a través de las funcionalidades de la plataforma, tales como la capacidad de descargar sus Datos Personales), y en cualquier caso en el plazo de 30 días desde la fecha de cese de cualquier Servicio que implique el Tratamiento de los Datos Personales del Cliente (la "**Fecha de Cese**"), y procurará aplicar lo mismo a todas las copias de dichos Datos Personales del Cliente.
- 9.2 Cada Encargado del Tratamiento Contratado puede conservar los Datos Personales del Cliente en la medida en que lo requiera la Legislación aplicable o según sea necesario para efectuar las operaciones de pago requeridas en virtud del Contrato, únicamente en la medida y durante el tiempo que exija la Legislación aplicable o que sea necesario para tales finalidades de pago, y siempre

que Soprano garantice la confidencialidad de todos los Datos Personales del Cliente y que estos se traten solamente para satisfacer los fines necesarios especificados en la Legislación aplicable que requieran su conservación, y no con otro objeto.

- 9.3 En el plazo de **30 días** desde la Fecha de Cese, Soprano facilitará al Cliente una certificación por escrito de que ha cumplido la presente cláusula 9 en su totalidad, previa solicitud por escrito de este.

10. Derechos de auditoría

- 10.1 Si la Legislación sobre Protección de Datos de la UE resulta de aplicación a los Datos Personales del Cliente, Soprano conviene en poner a disposición del Cliente, previa petición por escrito de este, toda la información necesaria a fin de demostrar el cumplimiento de la presente Adenda, asimismo permitirá y contribuirá a que el Cliente o un tercer auditor independiente debidamente cualificado encomendado por el Cliente, y corriendo este con los gastos, lleve a cabo auditorías, incluidas inspecciones, en relación con el Tratamiento de los Datos Personales del Cliente por parte de los Encargados Contratados.
- 10.2 Los derechos de información y auditoría del Cliente del apartado 10.1 podrán ejercerse en la medida en que el Contrato no otorgue de otra forma al Cliente los derechos de información y auditoría en cumplimiento de los requisitos pertinentes de la Legislación sobre Protección de Datos (incluyendo, cuando corresponda, el artículo 28(3)(h) del RGPD), y estarán sujetos a las condiciones indicadas en los apartados 10.3 y 10.4.
- 10.3 El Cliente notificará a Soprano, con un (1) mes de antelación como mínimo, cualquier auditoría o inspección que deba llevarse a cabo en virtud del apartado 10.1 y empleará todos los esfuerzos razonables (y procurará que cada uno de sus auditores así lo haga) para evitar causar cualquier daño, perjuicio (o minimizarlo en caso de no poder evitarlo) o interrupción en la actividad de Soprano durante el transcurso de dicha auditoría o inspección. Soprano no tiene obligación de facilitar acceso a información relevante a los efectos de dicha auditoría o inspección:
- 10.3.1 a ninguna persona física, salvo que esta proporcione pruebas adecuadas de su identidad y capacidad y esté sujeta a una obligación de confidencialidad;
- 10.3.2 fuera de su horario comercial habitual con el fin de llevar a cabo más de una auditoría o inspección en un año natural, excepto en el caso de cualquier auditoría o inspección que:
- 10.3.2.1 El Cliente considere razonablemente necesaria por tener inquietudes legítimas en cuanto al cumplimiento de la presente Adenda por parte de Soprano o de la Filial de Soprano en cuestión; o
- 10.3.2.2 La Legislación sobre Protección de Datos, una Autoridad de Control o cualquier otro organismo regulador de índole similar responsable de la aplicación de la Legislación sobre Protección

de Datos en cualquier país o territorio exija o solicite que una Filial Autorizada del Cliente la lleve a cabo,

siempre y cuando el Cliente haya plasmado sus inquietudes o la petición o requisito pertinente en su previa notificación por escrito remitida a Soprano para desarrollar la auditoría o inspección, y este último considere aceptables dichas inquietudes.

10.4 El Cliente acepta que su derecho a auditoría indicado anteriormente estará sujeto a las siguientes condiciones adicionales:

10.4.1 Soprano puede oponerse a cualquier tercer auditor nombrado por el Cliente en virtud del apartado 10.2 en caso de que, según el criterio razonable de Soprano, el auditor no sea independiente o no esté debidamente cualificado.

10.4.2 Antes de comenzar cualquier auditoría, el Cliente y Soprano abordarán y pactarán por adelantado la fecha de inicio razonable, el ámbito y la duración de la auditoría, además de los controles de seguridad y confidencialidad aplicables.

10.4.3 El Cliente reembolsará a Soprano todo coste relacionado en el que haya incurrido cualquier Encargado del Tratamiento Contratado para llevar a cabo cualesquiera auditorías o inspecciones con arreglo al apartado 10.1.

10.4.4 El Cliente, cuando efectúe una auditoría de conformidad con el apartado 10.1 en su propio nombre o en nombre de una Filial Autorizada del Cliente, empleará todos los esfuerzos razonables para combinar en una sola auditoría todas las peticiones para valorar el cumplimiento de la presente Adenda por parte de Soprano, minimizando así el impacto para este último. Para despejar cualquier duda, toda auditoría o inspección que la Filial Autorizada del Cliente desee llevar a cabo ante Soprano, la realizará exclusivamente el Cliente, tal y como se describe anteriormente, y Soprano cooperará únicamente en aquellas peticiones formuladas por el Cliente en nombre de dicha Filial.

11. Transferencias Restringidas

11.1 Por la presente, cada Filial Autorizada del Cliente (en calidad de "exportador de datos") y Soprano (en calidad de "importador de datos") formalizan las Cláusulas Contractuales Tipo en lo tocante a cualquier Transferencia Restringida de la Filial Autorizada del Cliente a Soprano, y dichas Cláusulas se incorporarán por referencia a esta Adenda y pueden ser aplicadas directamente por las Partes en la medida en que dichas transferencias estén sujetas a la Legislación sobre Protección de Datos de la UE y/o a la Legislación sobre Protección de Datos de UK.

11.2 Cuando la prestación de los Servicios implique una Transferencia Restringida, se aplicarán las Cláusulas Contractuales Tipo como se establece a continuación:

- i. Cuando una Filial Autorizada del Cliente actúe como Responsable, las Partes deberán cumplir con las **Cláusulas Tipo R-a-E de la UE**, sujetas a los términos adicionales de la Sección 1 del Anexo 2.
 - ii. Cuando una Filial Autorizada del Cliente actúe en calidad de Encargado del Tratamiento (incluyendo, sin limitación alguna, un Encargado en el sentido del artículo 28(4) del RGPD), las Partes deberán cumplir con las **Cláusulas Tipo E-a-E de la UE**, sujetas a los términos adicionales de la Sección 1 del Anexo 2, con el fin de proporcionar las garantías adecuadas a los Datos Personales del Cliente en nombre del correspondiente Responsable de dichos Datos.
- 11.3 Soprano declara y garantiza que, antes de iniciar cualquier Transferencia Restringida a un Subencargado, suscribirá las **Cláusulas Tipo E-a-E de la UE** establecidas en el Anexo 2 de esta Adenda, en nombre del Cliente o del Responsable de los Datos Personales del Cliente en cuestión, o garantizará de otro modo que dicha Transferencia Restringida se produce únicamente si se cumplen cualquiera de los siguientes requisitos: (i) dicha Transferencia Restringida se realiza conforme a una decisión de adecuación por parte de la Comisión o con otras garantías apropiadas de acuerdo con el Artículo 46 del RGPD, o (ii) con arreglo a las Normas Corporativas Vinculantes (BCRs) aprobadas por una Autoridad de Control competente de acuerdo con el Artículo 47 del RGPD, o (iii) se basa en las excepciones contempladas en el Artículo 49 del RGPD (y las garantías y/ o excepciones equivalentes a las que se hace referencia en el UK RGPD en relación con los Datos Personales originados en UK o sujetos a la Legislación sobre Protección de Datos de UK)..

12. Condiciones generales

Legislación aplicable y jurisdicción

- 12.1 Sin perjuicio de las cláusulas 7 (Mediación y jurisdicción) y 9 (Legislación aplicable) de las Cláusulas Contractuales Tipo:
- 12.1.1 por el presente, las partes de esta Adenda remiten su elección de jurisdicción a la estipulada en el Contrato con respecto a todo conflicto o reclamación que surja por cualquier causa en virtud de esta Adenda en lo referente a su existencia, validez, resolución o consecuencias de su nulidad; y
 - 12.1.2 la presente Adenda, todas las obligaciones no contractuales u otro tipo de obligaciones que se deriven o estén relacionadas con la misma se rigen por la legislación del país o territorio estipulado en el Contrato a estos efectos.

Orden de preferencia

- 12.2 Nada de lo dispuesto en esta Adenda limita las obligaciones de Soprano en virtud del Contrato en lo tocante a la protección de los Datos Personales, ni le permite tratar (o permitir el Tratamiento de) los Datos Personales de un modo que esté prohibido por el Contrato. Las Cláusulas Contractuales Tipo prevalecerán en caso de que surja cualquier conflicto o discrepancia entre las mismas y la presente

Adenda. Las condiciones de la Adenda tendrán preferencia sobre las condiciones del Contrato en caso de que surja cualquier conflicto entre ambos documentos.

- 12.3 Con sujeción al apartado 13.2, en lo que respecta al objeto de la presente Adenda, prevalecerán las disposiciones de la presente en caso de que surjan discrepancias entre las disposiciones de esta Adenda y cualesquiera otros acuerdos formalizados por las partes, incluyendo el Contrato y los acuerdos suscritos o supuestamente suscritos (salvo cuando se haya pactado explícitamente lo contrario por escrito y se haya firmado en nombre de las partes) después de la fecha de esta Adenda.

Modificaciones en la Legislación sobre Protección de Datos y otras disposiciones

- 12.4 El Cliente puede:

12.4.1 cuando lo considere oportuno y mediante notificación por escrito a Soprano con al menos 30 (treinta) días naturales de antelación, solicitar a Soprano cualquier modificación de las Cláusulas Contractuales Tipo (incluidas las Cláusulas Contractuales Tipo suscritas en virtud del apartado 11.1) en la medida en que resulten de aplicación a las Transferencias Restringidas sujetas a una Legislación sobre Protección de Datos concreta que, como resultado de cualquier cambio en, o por decisión de una autoridad competente en virtud de dicha Legislación, la modificación solicitada sea necesaria para permitir que se lleven a cabo (o que continúen llevándose a cabo) tales Transferencias Restringidas sin contravenir dicha Legislación sobre Protección de Datos; y

12.4.2 proponer cualquier otra modificación a la presente Adenda que el Cliente considere razonablemente necesaria para satisfacer los requisitos de cualquier Legislación sobre Protección de Datos.

- 12.5 Si el Cliente remite una notificación con arreglo al apartado 13.4.1, Soprano cooperará sin demora (y procurará que cualquier Subencargado afectado coopere rápidamente) para garantizar que se apliquen las modificaciones equivalentes a cualquier acuerdo formalizado en virtud del apartado 5.4.1.

- 12.6 Si el Cliente remite una notificación con arreglo al apartado 13.4.2, las partes abordarán de manera inmediata las modificaciones propuestas y las negociarán de buena fe con vistas a acordar e implementar las mismas u otras alternativas para satisfacer los requisitos señalados en la notificación del Cliente tan pronto como sea razonablemente factible.

- 12.7 El Cliente no requerirá el consentimiento o la aprobación de ninguna Filial del Cliente, que actúe como Filial Autorizada del Cliente, para modificar la presente Adenda con arreglo a este apartado 13 u otro apartado, y garantizará que las respectivas Filiales del cliente han proporcionado todas las autorizaciones necesarias.

Divisibilidad

- 12.8 En caso de que alguna disposición de la presente Adenda resulte nula o no aplicable, el resto de la Adenda seguirá siendo válida y vigente. La disposición

nula o no aplicable (i) se modificará según sea necesario para garantizar su validez y aplicabilidad, preservando las intenciones de las partes de la forma más fiel posible o, si esto no es factible, (ii) se interpretará como si la parte nula o no aplicable nunca hubiera estado contenida en la misma.

Las Partes del presente han formalizado esta Adenda mediante sus representantes debidamente autorizados suscribiendo el Contrato pertinente, que hace referencia a la Adenda en la fecha indicada en el mismo.

ANEXO 1: INFORMACIÓN SOBRE EL TRATAMIENTO DE LOS DATOS PERSONALES DEL CLIENTE

El presente Anexo 1 incluye cierta información sobre el Tratamiento de los Datos Personales del Cliente según lo exige el Artículo 28(3) del RGPD:

- **Objeto y duración del tratamiento.**

El objeto del Tratamiento de los Datos Personales del Cliente por parte de Soprano es la prestación de los Servicios establecidos en el Contrato. Los Datos Personales del Cliente se tratarán durante el periodo de vigencia del Contrato, con sujeción a las disposiciones de la presente Adenda.

- **Naturaleza y finalidad del tratamiento.**

La naturaleza y finalidad del tratamiento será la prestación de servicios de telecomunicaciones para enviar mensajes electrónicos, tal y como se especifica con más detalle en el Contrato.

- **Operaciones de tratamiento.**

Los Datos Personales estarán sujetos a las siguientes actividades básicas de tratamiento: Remisión a los proveedores de telecomunicación para su entrega; conservación; acceso para los Servicios de atención al cliente; detección, prevención y corrección de mensajes y correos electrónicos abusivos; supervisión, mantenimiento y mejora de los Servicios.

- **Tipos de Datos Personales del Cliente a tratar.**

El Cliente ejerce pleno control sobre los Datos Personales que se transfieren a Soprano. Los Datos personales pueden incluir, entre otros, los siguientes tipos:

- Información de contacto (números de teléfono, direcciones de correo electrónico)
- Datos de identificación (nombre y apellidos)
- Datos de tráfico (IMEI, IMSI, MSISDN...)
- Contenido intercambiado mediante el uso de los Servicios, como texto, cuerpos de mensaje, medios de voz y vídeo, imágenes y sonido.
- Cualesquiera otros Datos Personales facilitados por el Cliente.

- **Categorías especiales de datos**

Soprano no pretende recopilar ni tratar intencionadamente categorías especiales de datos en la prestación de sus Servicios y, por lo tanto, las Filiales Autorizadas del Cliente se comprometen a no transmitir datos de dicha índole a los Subencargados Contratados. No obstante, ya que las Filiales Autorizadas del Cliente ejercen un control total sobre los Datos Personales que se transfieren a los Encargados Contratados, dichas Filiales son las únicas responsables de la licitud del tratamiento de cualquier categoría especial de datos que los Encargados Contratados traten de forma involuntaria.

- **Categorías de Interesados**

Los Interesados pueden incluir clientes, empleados, proveedores y usuarios finales del Cliente que sean personas físicas, cuyos datos se proporcionan a los Encargados del Tratamiento Contratados a través de los Servicios por parte de o bajo la dirección de las Filiales Autorizadas del Cliente o por los clientes del Cliente;

- **Información de contacto**

Si tiene alguna pregunta, puede ponerse en contacto con el Departamento de Privacidad de Soprano en Privacy@sopranodesign.com

ANEXO 2: CLÁUSULAS CONTRACTUALES TIPO

Antecedentes

El exportador de datos ha suscrito esta Adenda con el importador de datos. De conformidad con los términos de la Adenda, se contempla que los Servicios prestados por el importador de datos impliquen la transferencia de Datos Personales al importador de datos. El importador de datos se encuentra en un país que no garantiza un nivel adecuado de protección de datos perseguido por la Legislación sobre Protección de Datos de la UE y de UK. Para garantizar el cumplimiento del UE RGPD, UK RGPD y la Legislación sobre Protección de Datos de la UE u de UK aplicables, el Responsable del Tratamiento acepta la prestación de dichos Servicios, incluido el tratamiento de datos personales incidentales a los mismos, sujeto a la ejecución y al cumplimiento por parte del importador de datos de estas Cláusulas Contractuales Tipo (en adelante, "CCTs").

A los efectos de las Cláusulas Tipo R-a-E de la UE y las Cláusulas Tipo E-a-E de la UE, la Filial Autorizada del Cliente es el exportador de datos y Soprano es el importador de datos. Cuando el presente Anexo 2 no mencione explícitamente las Cláusulas Tipo R-a-E de la UE o las Cláusulas Tipo E-a-E de la UE, se aplicará a ambas.

1. CLÁUSULAS OPERATIVAS DE LAS CCTs Y TÉRMINOS ADICIONALES

- 1.1. Incorporación por referencia y prevalencia.** las disposiciones de las CCTs se incorporan por referencia al Contrato. Si existieran contradicciones entre el contenido de las CCTs y el contenido del Contrato, se deberá dar preferencia a las disposiciones de las CCTs. Si existieran contradicciones entre el contenido de las UE CCTs y el contenido de las UK CCTs, se deberá dar preferencia a las disposiciones de las UK CCTs en la medida en que sean aplicables a la Transferencia Restrictada.
- 1.2. Cláusula de incorporación.** Se aplicará la opción prevista en la cláusula 7.
- 1.3. Supresión o devolución de datos.** Las Partes acuerdan que la obligación de suprimir o devolver los Datos Personales del Cliente se aplicará en la medida en que los Datos Personales del Cliente no se hayan facilitado previamente ni se hayan puesto a disposición de la Filial Autorizada del Cliente a través de las funcionalidades de la plataforma, tales como la capacidad de descargar los Datos Personales del Cliente. Las partes también acuerdan que la acreditación de supresión de los Datos Personales del Cliente requerida en la cláusula 8.5 y 16 (d) de las CCTs será facilitada por Soprano previa solicitud por escrito del Cliente.
- 1.4. Autorización general para recurrir a subencargados.** Será de aplicación la opción 2 de la cláusula 9 (a) de conformidad con lo dispuesto en la Cláusula 5 del DPA, incluyendo lo referente al plazo de notificación previa de cualquier cambio en los subencargados.
- 1.5. Derechos del interesado.** A los efectos de la cláusula 10 de las Cláusulas Tipo E-a-E de la UE, y sujeto a lo establecido en la Cláusula 6 del DPA, Soprano notificará al

Cliente cualquier solicitud que haya recibido de un interesado, y el Cliente deberá notificarlo al Responsable correspondiente, según corresponda.

1.6. Reparación. El clausulado opcional de la Cláusula 11 no será de aplicación.

1.7. Supervisión. La cláusula 13 (a) se aplicará de la siguiente manera:

1.7.1 Cuando la Filial Autorizada del Cliente esté establecida en un Estado miembro de la UE: La autoridad de control responsable de garantizar que el exportador de datos cumpla el Reglamento (UE) 2016/679 en cuanto a la transferencia de los datos, indicada en el anexo I.C, actuará como autoridad de control competente.

1.7.2 Cuando la Filial Autorizada del Cliente no esté establecida en un Estado miembro de la UE, pero sí en un lugar que entre dentro del ámbito territorial de aplicación del Reglamento (UE) 2016/679, de conformidad con el artículo 3, apartado 2, y haya nombrado a un representante con arreglo al artículo 27, apartado 1, del Reglamento (UE) 2016/679: La autoridad de control del Estado miembro en que esté establecido el representante en el sentido del artículo 27, apartado 1, del Reglamento (UE) 2016/679, indicada en el anexo I.C, actuará como autoridad de control competente.

1.7.2 Cuando la Filial Autorizada del Cliente no esté establecida en un Estado miembro de la UE, pero sí en un lugar que entre dentro del ámbito territorial de aplicación del Reglamento (UE) 2016/679 de la Comisión, de conformidad con el artículo 3, apartado 2, y no haya nombrado a un representante con arreglo al artículo 27, apartado 2, del Reglamento (UE) 2016/679 de la Comisión: Agencia Española de Protección de Datos (AEPD)- C/ Jorge Juan, 6, 28001 Madrid, actuará como autoridad de control competente.

1.7.4 Cuando la Filial Autorizada del Cliente esté establecida en el Reino Unido o entre dentro del ámbito de aplicación territorial de la Legislación sobre Protección de Datos de UK: el UK Information Commissioner's Office (ICO) actuará como autoridad de control competente.

1.8. Derecho aplicable. A los efectos de la cláusula 17, la ley aplicable será la ley establecida en el Contrato. Si el Contrato no se rige por la legislación de un Estado Miembro de la UE, las CCTs se regirán por: (i) las leyes de España; o (ii) cuando el Contrato esté sujeto a las leyes del Reino Unido o los Datos Personales se exporten desde el Reino Unido, las CCTs se regirán por las leyes del Reino Unido.

1.9. Foro y jurisdicción. A los efectos de la cláusula 18, los tribunales competentes para resolver cualquier disputa que surja de las CCTs serán los establecidos en el Contrato. Si el Contrato no designa a un tribunal de un Estado Miembro de la UE con jurisdicción exclusiva para resolver cualquier disputa que surja de este Contrato, las Partes acuerdan que los tribunales de España tendrán jurisdicción exclusiva para resolver cualquier disputa que surja de las CCTs, excepto cuando el Contrato se rija por las leyes del Reino Unido o cuando los Datos Personales se exporten desde el Reino Unido, en cuyo caso las Partes se someten a la jurisdicción exclusiva de los tribunales ingleses para resolver cualquier disputa que surja de las CCTs.

APÉNDICE

ANEXO I

A. LISTA DE PARTES

Exportador(es) de datos: *[Identidad y datos de contacto del exportador o exportadores de datos y, en su caso, del delegado de protección de datos de este o estos y/o del representante en la Unión Europea]*

Nombre: Filiales Autorizadas del Cliente identificadas en el Contrato pertinente a través del cual se suscribe la presente Adenda, y según proceda de conformidad con la cláusula 11.1 de la Adenda (el Cliente ha suscrito esta Adenda, incluyendo las Cláusulas Contractuales Tipo, en su propio nombre y en el de cada Filial del Cliente que actúa como Filial Autorizada del Cliente, según corresponda de conformidad con la cláusula 11.1 de esta Adenda)

Dirección: Las direcciones de las Filiales Autorizadas del Cliente identificadas en el Contrato pertinente a través del cual se suscribe la presente Adenda.

Nombre, cargo y datos de contacto de la persona de contacto: Los datos de contacto de las Filiales Autorizadas del Cliente identificadas en el Contrato pertinente a través del cual se suscribe la presente Adenda.

Actividades relacionadas con los datos transferidos en virtud del presente pliego de cláusulas: La prestación de Servicios, tal y como se especifica con más detalle en el Contrato

Firma y fecha:

Función (responsable/encargado): A los efectos de las Cláusulas Tipo R-a-E de la UE, la Filial Autorizada del Cliente actúa como Responsable. A los efectos de las Cláusulas Tipo E-a-E de la UE, la Filial Autorizada del Cliente actúa como Encargado.

Importador(es) de datos: *[Identidad y datos de contacto del importador o importadores de datos, incluida cualquier persona de contacto responsable de la protección de los datos]*

Nombre: La entidad Soprano descrita en el Contrato pertinente.

Dirección: La dirección de Soprano descrita en el Contrato pertinente.

Nombre, cargo y datos de contacto de la persona de contacto: privacy@sopranodesign.com

Actividades relacionadas con los datos transferidos en virtud del presente pliego de cláusulas: La prestación de Servicios, tal y como se especifica con más detalle en el Contrato.

Firma y fecha:

Función (responsable/encargado): Encargado.

B. DESCRIPCIÓN DE LA TRANSFERENCIA DE LOS DATOS PERSONALES RELEVANTES

- **Categorías de interesados cuyos datos personales se transfieren**

Según descrito en el Anexo 1 del DPA.

- **Categorías de Datos Personales del Cliente transferidos**

Según descrito en el Anexo 1 del DPA.

- **Datos sensibles transferidos (si procede)**

Según descrito en el Anexo 1 del DPA.

- **Frecuencia de la transferencia**

Periódica.

- **Naturaleza del tratamiento**

La naturaleza del tratamiento será la prestación de Servicios, tal y como se especifica con más detalle en el Contrato

Finalidad(es) de la transferencia y posterior tratamiento de los datos

La finalidad del tratamiento será la prestación de servicios de telecomunicaciones para enviar mensajes electrónicos, tal y como se especifica con más detalle en el Contrato y en la página web del importador de datos <https://www.sopranodesign.com/>.

- **Operaciones de Tratamiento.**

Los Datos Personales estarán sujetos a las siguientes actividades básicas de tratamiento: Remisión a los proveedores de telecomunicación para su entrega; conservación; acceso para los Servicios de atención al cliente; detección, prevención y corrección de mensajes y correos electrónicos abusivos; supervisión, mantenimiento y mejora de los Servicios.

- **Duración del Tratamiento.**

El plazo durante el cual se conservarán los datos personales o, cuando eso no sea posible, los criterios utilizados para determinar este plazo

Los Datos Personales del Cliente se tratarán durante el periodo de vigencia del Contrato, con sujeción a las disposiciones de la presente Adenda.

- **Transferencia a (sub)encargados**

En caso de transferencia a (sub)encargados, especifíquese también el objeto, la naturaleza y la duración del tratamiento

Los subencargados tratarán los Datos Personales del Cliente según sea necesario para prestar los Servicios de conformidad con el Contrato y durante la vigencia del Contrato. El exportador de datos mantiene un listado actualizado de sus subencargados y respectivas ubicaciones que se pondrá a disposición del importador de datos previa solicitud por escrito, de conformidad con lo establecido en la Cláusula 5 del DPA.

C. AUTORIDAS DE CONTROL COMPETENTE

Indíquese la autoridad o autoridades de control competentes de conformidad con la cláusula 13

- Cuando el exportador de datos esté establecido en un Estado miembro de la UE: La autoridad de control responsable de garantizar que el exportador de datos cumpla el Reglamento (UE) 2016/679 en cuanto a la transferencia de los datos, indicada en el anexo I.C, actuará como autoridad de control competente.
- Cuando el exportador de datos no esté establecido en un Estado miembro de la UE, pero sí en un lugar que entre dentro del ámbito territorial de aplicación del Reglamento (UE) 2016/679, de conformidad con el artículo 3, apartado 2, y haya nombrado a un representante con arreglo al artículo 27, apartado 1, del Reglamento (UE) 2016/679: La autoridad de control del Estado miembro en que esté establecido el representante en el sentido del artículo 27, apartado 1, del Reglamento (UE) 2016/679, indicada en el anexo I.C, actuará como autoridad de control competente.
- Cuando el exportador de datos no esté establecido en un Estado miembro de la UE, pero sí en un lugar que entre dentro del ámbito territorial de aplicación del Reglamento (UE) 2016/679 de la Comisión, de conformidad con el artículo 3, apartado 2, y no haya nombrado a un representante con arreglo al artículo 27, apartado 2, del Reglamento (UE) 2016/679 de la Comisión: Agencia Española de Protección de Datos (AEPD)- C/ Jorge Juan, 6, 28001 Madrid, actuará como autoridad de control competente.
- Cuando el exportador de datos esté establecido en el Reino Unido o entre dentro del ámbito de aplicación territorial de la Legislación sobre Protección de Datos de UK: el UK Information Commissioner's Office (ICO) actuará como autoridad de control competente.

ANEXO II- MEDIDAS TÉCNICAS Y ORGANIZATIVAS, EN ESPECIAL MEDIDAS TÉCNICAS Y ORGANIZATIVAS PARA GARANTIZAR LA SEGURIDAD DE LOS DATOS

DESCRIPCIÓN GENERAL DE LA SEGURIDAD EN SOPRANO

1. Esta visión general establece los elementos clave de Soprano de su sistema de gestión de seguridad de la información (SGSI) y sus controles de seguridad técnicos y organizativos.

2. SGSI DE SOPRANO. El SGSI de Soprano se adhiere al marco del Sistema de Gestión de Seguridad de la Información ISO27001. El SGSI de Soprano es supervisado y administrado por un comité directivo ejecutivo de seguridad (compuesto por el CEO y el CTO) que revisa regularmente los procesos y procedimientos con el equipo de seguridad de Soprano. Soprano ha establecido roles de seguridad y cumplimiento y una matriz de responsabilidad como parte crítica de sus operaciones. Además de la auditoría anual requerida para la

certificación ISO27001, tenemos un programa de auditorías internas para garantizar el cumplimiento.

3. Seguridad del personal. Soprano realiza verificaciones de antecedentes de sus empleados en el momento de la contratación de acuerdo con las leyes locales. Los controles se basan en la naturaleza y el alcance de la función pertinente y pueden incluir la verificación del empleo y la educación, las verificaciones de referencias, las comprobaciones penales y de inmigración. Todo el personal debe realizar formaciones de seguridad al menos una vez al año y realizamos pruebas de phishing regularmente. Se requiere que todo el personal lea y reconozca las políticas de seguridad clave como parte del proceso de incorporación a la empresa. También tenemos una política de denuncia de irregularidades (política de *whistleblowing*) que alienta a nuestro personal a denunciar cualquier comportamiento poco ético.

4. Gestión de activos. Tenemos una política de gestión de activos que incluye un requisito para los registros de activos y un enfoque estandarizado para la eliminación de datos y la destrucción de activos como parte del desmantelamiento. Contamos con un sistema de gestión de Tecnologías de la Información (IT) centralizado que garantiza que todo el software y hardware utilizado por nuestro personal debe ser aprobado por nuestro equipo de IT. Los discos duros de las computadoras están encriptados y se pueden borrar de forma remota. Nuestra política BYOD (de sus siglas en inglés "*Bring Your Own Device*") restringe el acceso a los datos de la empresa y evita la captura de datos de la empresa en dispositivos personales.

3. Control de acceso. Soprano aplica el control de acceso basado en roles ("*RBAC*" o *Role Based Access Control*) combinado con el principio de mínimos privilegios para el acceso del personal a los datos de los clientes. El acceso del personal está sujeto a 2FA (autenticación de dos factores). El acceso se revisa automáticamente cuando un miembro del personal cambia de rol o abandona la organización, así como durante las auditorías programadas dos veces al año. Mantenemos una política de contraseñas para garantizar una complejidad de contraseña adecuada y minimizar la posibilidad de compromiso. Las contraseñas almacenadas en nuestros sistemas se cifran mediante *hash*. Se registran todos los eventos de inicio de sesión. Las cuentas de usuario tienen un ID de usuario único y nunca se reutilizan.

4. Cifrado. Soprano cifra (a) todas las bases de datos que almacenan datos de clientes en reposo (AES256); (b) Datos del Cliente en tránsito entre la aplicación del Cliente y su Plataforma (TLS 1.2 para comunicaciones para el acceso al portal web y para las API aplicables). Mantenemos políticas que cubren la gestión de las claves de cifrado desde la generación hasta la expiración o terminación.

5. Seguridad física. La política de seguridad física de Soprano garantiza que se tomen las medidas adecuadas para salvaguardar la seguridad de las oficinas de Soprano. Nos aseguramos de que los proveedores de alojamiento de datos administrados por terceros que utilizamos tengan controles de seguridad física que cumplan con las mejores prácticas y sean auditados de forma independiente anualmente.

6. Seguridad de las operaciones. Aplicamos una política estándar de control de cambios que incluye procedimientos de prueba, aprobación, control de versiones y reversión. Todos los servidores que alojan nuestros productos son versiones reforzadas del sistema operativo. Utilizamos herramientas antimalware, antivirus, IDS e IPS para proteger nuestra infraestructura. Los registros de seguridad se conservan durante al menos 12 meses. Nuestras plataformas se monitorean internamente a través de herramientas de sistemas de gestión de eventos y alertas.

7. Gestión de vulnerabilidades y pruebas de penetración. Soprano gestiona las vulnerabilidades de acuerdo con una política escrita para mitigar cualquier riesgo identificado. Soprano utiliza herramientas de terceros para realizar escaneos regulares de su plataforma. Aplica parches de software basados en marcos de tiempo determinados por referencia a la criticidad de la vulnerabilidad. Los parches se evalúan y prueban antes de la implementación. Contratamos a terceros independientes para llevar a cabo escaneos de vulnerabilidades al menos una vez cada doce meses en nuestras plataformas. Las amenazas y vulnerabilidades detectadas se evalúan, clasifican y subsanan de acuerdo con nuestra política de gestión de vulnerabilidades.

8 Seguridad de las comunicaciones de datos. Si bien algunos de nuestros sistemas están dedicados a un solo cliente, la mayoría son multiusuario (*multi-tenanted*), con separación lógica aplicada para cada cliente. Mantenemos una arquitectura técnica de 3 niveles con servicios de firewall completamente funcionales en cada límite de nivel. Nuestros servidores que proporcionan servicios externos, como servicios de portal y API, se encuentran en zonas DMZ. Se utiliza VPN para acceder a los sistemas de producción de forma remota, con 2FA y cifrado a través de TLS.

9 Adquisiciones, Desarrollo y Mantenimiento de Sistemas. Hemos desarrollado nuestro Ciclo de Vida de Desarrollo de Software de acuerdo con ISO27001 para garantizar la seguridad de las nuevas versiones y funcionalidades. Nuestra plataforma está desarrollada para tener en cuenta las diez principales vulnerabilidades de OSWASP. Todos los componentes de código abierto se escanean utilizando un software de escaneo de terceros antes de la implementación. Mantenemos la separación de "espacio de aire" entre nuestros entornos de pre- y producción. No se utilizan datos de clientes en nuestros entornos de preproducción. El código fuente está protegido a través de un servicio de alojamiento de repositorio de código fuente de terceros y el acceso está limitado según la función del trabajo.

10. Gestión de la seguridad de los proveedores. Contamos con políticas y procesos para garantizar que los riesgos de seguridad de los proveedores sean identificados, monitoreados y administrados. Para nuestros proveedores de alojamiento externos, por ejemplo, esto incluye una revisión anual de los informes de auditoría de seguridad independientes y el logro del nivel de servicio.

11. Seguridad en la nube. Nuestros servicios se alojan en servidores gestionados dedicados en centros de datos con certificación ISO27001, gestionados por proveedores externos de

confianza. Los datos se cifran en reposo y los proveedores de alojamiento no pueden acceder a ellos. Nuestros proveedores de alojamiento proporcionan servicios de seguridad gestionados que incluyen IDS, IPS, protección DDoS y servicios antimalware. Contamos con procesos y sistemas para detectar comportamientos de red sospechosos o inusuales y para apoyar la investigación forense en caso de violación de la seguridad.

12. Gestión de incidencias. Soprano mantiene una política y planes de gestión de incidentes para garantizar que los incidentes de seguridad relevantes se gestionen de manera rápida y eficaz, y que abordemos cualquier causa raíz. Soprano tiene un equipo de gestión de incidentes multidisciplinario al que se le notifica automáticamente cualquier incidente a través de una herramienta *online*. Los incidentes se comunican rápidamente a los clientes de acuerdo con las obligaciones contractuales y la ley aplicable.

13. Continuidad del negocio, DR y Backup. Tenemos un plan de continuidad del negocio para responder a cualquier interrupción significativa del negocio, que se revisa anualmente. También realizamos análisis de impacto en el negocio para funciones clave. Para cada región en la que opera, la plataforma de software de Soprano está alojada en centros de datos geográficamente separados con replicación de datos que proporciona disponibilidad para fallas parciales y completas del sitio. Como protección adicional, se realizan copias de seguridad separadas de nuestra base de datos en nuestro sitio de recuperación de desastres (DR). Como resultado de estas medidas, podemos lograr una recuperación puntual de datos y alcanzar objetivos de servicio definidos, RTO y RPO. Testeamos nuestros planes de recuperación de datos anualmente.

15. Cumplimiento. La auditoría interna y externa de nuestro SGSI se lleva a cabo como parte de nuestra certificación ISO27001:2013. Colaboramos con terceros para realizar análisis anuales de vulnerabilidades y análisis automatizados de nuestras plataformas. Tenemos un proceso para identificar los requisitos regulatorios en cada jurisdicción en la que operamos y nuestro equipo legal evalúa el cumplimiento de la legislación clave como el RGPD.

Certificación:

ISO27001:2013 (plataformas australianas, británicas y neozelandesas)

Cyber Essentials Plus (TI corporativa)

[ANEXO III – LISTA DE SUBENCARGADOS DEL TRATAMIENTO](#)

No procede.

Última actualización; 3 Agosto, 2022.