Cláusulas contractuales tipo

A los efectos del artículo 28, apartado 3, del Reglamento 2016/679 (el RGPD)

El cliente
(el “**responsable del tratamiento de datos**”)

y

SameSystem A/S
CVR/IVA N°: 31487927
Rentemestervej 2A
2400 København NV
Dinamarca
(el “**encargado del tratamiento de datos**”)

cada uno como "parte"; y juntos como las "partes"

HAN ACORDADO las siguientes Cláusulas Contractuales (las Cláusulas) para cumplir con los requisitos del RGPD y para garantizar la protección de los derechos del interesado. Estas Cláusulas forman parte del acuerdo de licencia entre las partes.

Las presentes Cláusulas regirán el tratamiento de los datos personales realizado por el encargado del tratamiento (incluidas sus filiales) en nombre del responsable del tratamiento (incluidas sus filiales).

1. Índice

2. Preámbulo

1. Las presentes Cláusulas Contractuales (las Cláusulas) establecen los derechos y obligaciones del responsable del tratamiento y del encargado del tratamiento cuando procesa datos personales en nombre del responsable del tratamiento.

2. Las Cláusula han sido diseñadas para garantizar que las partes cumplan con el artículo 28, apartado 3, del Reglamento 2016/679 del Parlamento Europeo y del Consejo del 27 de abril de 2016 sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos y por el que se deroga la Directiva 95/46/EC (Reglamente General de Protección de Datos).

3. El encargado del tratamiento prestará los servicios descritos en el acuerdo de licencia y en las condiciones generales de la licencia entre las partes y, con el fin de cumplir con el acuerdo de licencia, tratará los datos personales en nombre del responsable del tratamiento según las Cláusulas.

4. El presente acuerdo de tratamiento de datos sustituirá a todos los acuerdos de tratamiento anteriores entre el encargado y el responsable del tratamiento.

5. Se adjuntan cuatro anexos a estas Cláusulas y son parte integral de las mismas.

6. El Anexo A contiene detalles sobre el tratamiento de los datos personales, inclusive la finalidad y la naturaleza del tratamiento, el tipo de datos personales, las categorías de los interesados y la duración del tratamiento.

7. El Anexo B contiene las condiciones del responsable del tratamiento para el uso de subencargados por parte del encargado del tratamiento, así como una lista de subencargados autorizados por el responsable del tratamiento.

8. El Anexo C contiene las instrucciones del responsable en relación con el tratamiento de los datos personales, las medidas de seguridad mínimas que debe implementar el encargado del tratamiento y cómo deben realizarse las auditorías del encargado y de los subencargados del tratamiento.

9. El Anexo D contiene disposiciones sobre otras actividades que no están contempladas en las Cláusulas.

10. Ambas partes deben conservar las Cláusulas junto con los anexos por escrito, así como en formato electrónico.

11. Las Cláusulas no eximirán al encargado del tratamiento de las obligaciones a las que esté sujeto en virtud del Reglamento General de Protección de Datos (el RGPD) u otra norma.

3. Derechos y obligaciones del responsable del tratamiento

1. El responsable del tratamiento está a cargo de garantizar que el tratamiento de los datos personales se realice de conformidad con el RGPD (véase el artículo 24 del RGPD), las disposiciones vigentes de la UE o de los Estados Miembros [1]sobre la protección de datos y las presentes Cláusulas.

2. El responsable del tratamiento tiene el derecho y la obligación de toma decisiones sobre los fines y los medios del tratamiento de datos personales.

[1] Las referencias a los "Estados Miembros" a lo largo de las Cláusulas se entenderán como referencias a los "Estados Miembros de EEE".

3. El responsable del tratamiento tendrá la responsabilidad, entre otras cosas, de garantizar que el tratamiento de los datos personales que deberá realizar el encargado tenga un fundamento legal.

4. El encargado del tratamiento actúa según las instrucciones

1. El encargado del tratamiento solo tratará los datos personales siguiendo las instrucciones documentadas del responsable del tratamiento, salvo que así lo exija las leyes de la Unión o de los Estados Miembros a las que esté sujeto el encargado. Dichas instrucciones se especificarán en los anexos A y C. El responsable del tratamiento podrá dar instrucciones posteriores mientras dure el tratamiento de los datos personales, pero estas instrucciones siempre deben estar documentadas y establecidas por escrito, además de ser almacenadas en formato electrónico, en relación con las Cláusulas.

2. El encargado del tratamiento informará de inmediato al responsable del tratamiento si las instrucciones dadas por este último, en la opinión del encargado, contradicen el RGPD o las disposiciones vigentes sobre la protección de datos de la UE o de los Estados Miembros.

5. Confidencialidad

1. El encargado del tratamiento solo concederá acceso a los datos personales que se estén tratando en nombre del responsable del tratamiento a las personas que estén bajo la autoridad del encargado del tratamiento y que se hayan comprometido a mantener la confidencialidad o que estén sujetas a una obligación legal adecuada de confidencialidad y solo cuando sea necesario. La lista de personas a las que se ha concedido el acceso se revisará periódicamente. Basada en dicha revisión, el acceso a los datos personales se puede revocar si ya no es necesario, y en consecuencia, estas personas dejarán de tener acceso a los datos personales.

2. El encargado del tratamiento demostrará, a petición del responsable del tratamiento, que las personas implicadas que están bajo su autoridad están sujetas a la confidencialidad antes mencionada.

6. Seguridad del tratamiento

1. El artículo 32 del RGPD establece que, teniendo en cuenta los avances tecnológicos, los costos de implementación y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como el riesgo de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento implementarán las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.

   El responsable del tratamiento evaluará los riesgos para los derechos y libertades de las personas físicas inherentes al tratamiento e implementará medidas para mitigarlos. Dependiendo de su relevancia, las medidas pueden incluir lo siguiente:
   a. Uso de seudónimos y cifrado de datos personales;

   b. la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resistencia permanentes de los sistemas y servicios de tratamiento;

   c. la capacidad de restablecer la disponibilidad y el acceso a los datos personales de manera oportuna en caso de un incidente físico o técnico;

d. un proceso para comprobar, valorar y evaluar periódicamente la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. De acuerdo con el artículo 32 del RGPD, el encargado del tratamiento también deberá -independientemente del responsable del tratamiento- evaluar los riesgos para los derechos y libertades de las personas físicas inherentes al tratamiento e implementar medidas para mitigar dichos riesgos. A tal efecto, el responsable del tratamiento facilitará al encargado del tratamiento toda la información necesaria para identificar y evaluar los riesgos.

3. Además, el encargado del tratamiento asistirá al responsable del tratamiento para garantizar que este último cumple con las obligaciones en virtud del artículo 32 del RGPD, *entre otras cosas*, proporcionando al responsable del tratamiento información relativa a las medidas técnicas y organizativas ya implementadas por el encargado del tratamiento según lo establecido en el artículo 32 del RGPD, junto con toda la información adicional necesaria para que el responsable del tratamiento cumpla con su obligación.

   Si posteriormente - en la evaluación del responsable del tratamiento - la mitigación de los riesgos identificados requiere que el encargado del tratamiento implemente medidas adicionales a las ya implementadas por el mismo en virtud del artículo 32 del RGPD, el responsable del tratamiento especificará en el Anexo C estas medidas adicionales que deberán implementarse.

7. Uso de subencargados

1. El encargado del tratamiento cumplirá con los requisitos especificados en el artículo 28, apartados 2 y 4 del RGPD para poder contratar a otro encargado del tratamiento (un subencargado).

2. Por lo tanto, el encargado del tratamiento no contratará a otro encargado (subencargado) para el cumplimiento de las Cláusulas sin la autorización general previa por escrito del responsable del tratamiento.

3. El encargado del tratamiento cuenta con la autorización general del responsable del tratamiento para la contratación de subencargados. El encargado del tratamiento informará por escrito al responsable del tratamiento de cualquier cambio previsto en relación con la adición o sustitución de subencargados con un mínimo de 30 días de antelación, dando así al responsable del tratamiento la oportunidad de oponerse a dichos cambios antes de la contratación del subencargado(s) en cuestión. En el anexo B se pueden facilitar plazos más largos de notificación previa para servicios específicos por parte de subencargados. La lista de subencargados que cuentan con la autorización del responsable del tratamiento se puede encontrar en el anexo B.

4. Cuando el encargado del tratamiento contrate a un subencargado para realizar tareas específicas de tratamiento en nombre del responsable del tratamiento, se impondrán a dicho subencargado las mismas obligaciones de protección de los datos que se establecen en las Cláusulas mediante un contrato u otro acto jurídico en virtud de la legislación de la UE o de los Estados Miembros, en particular que proporcionen garantías suficientes para implementar las medidas técnicas y organizativas adecuadas de tal manera que el tratamiento cumpla con los requisitos de las Cláusulas y del RGPD.

   Por lo tanto, el encargado del tratamiento será responsable de exigir que el subencargado cumpla como mínimo con las obligaciones a las que está sujeto el encargado del tratamiento en función de las Cláusulas y del RGPD.

5. A petición del responsable del tratamiento, se le presentará una copia de dicho acuerdo de subencargado y de las modificaciones posteriores, lo que dará al responsable del tratamiento la oportunidad de garantizar que el subencargado esté sujeto a las mismas obligaciones de protección de datos que se establecen en las Cláusulas. Las cláusulas sobre cuestiones relacionadas con el negocio que no afecten al contenido legal de la protección de datos del acuerdo de subencargado no requieren ser presentadas al responsable del tratamiento.

6. Si el subencargado no cumple sus obligaciones en cuanto a la protección de datos, el encargado del tratamiento seguirá teniendo plena responsabilidad ante el responsable del tratamiento en lo que respecta al cumplimiento de las obligaciones del subencargado. Esto no afecta los derechos de los interesados en virtud del RGPD, en particular los previstos en los artículos 79 y 82 del Reglamento, contra el responsable del tratamiento y el encargado del tratamiento, incluido el subencargado.

8. Transferencia de datos a terceros países u organizaciones internacionales

1. Toda transferencia de datos personales a terceros países u organizaciones internacionales por parte del encargado del tratamiento se producirá únicamente de acuerdo con instrucciones documentadas del responsable del tratamiento y siempre deberá cumplir con el capítulo 5 del RGPD.

2. En caso de que las transferencias a terceros países u organizaciones internacionales, las cuales el responsable del tratamiento no haya ordenado realizar al encargado del tratamiento, sean requeridas en virtud de la legislación de la UE o de los Estados Miembros a la que esté sujeto el encargado del tratamiento, este informará al responsable del tratamiento de dicho requerimiento legal antes del tratamiento, a menos que la legislación mencionada prohíba la información por motivos importantes de interés público.

3. Por lo tanto, sin instrucciones documentadas del responsable del tratamiento, el encargado del tratamiento no podrá en el marco de las Cláusulas:

    a. transferir datos personales a un responsable o encargado del tratamiento en un tercero país u organización internacional

    b. transferir el tratamiento de los datos personales a un subencargado en un tercer país

    c. hacer que los datos personales sean tratados por el encargado del tratamiento en un tercer país

4. En el anexo C, sección 6, se establecerán las instrucciones del responsable del tratamiento relacionadas con la transferencia de datos personales a un tercer país incluído, si corresponde, el instrumento de transferencia según el capítulo 5 del RGPD en el cual se basan.

5. Las Cláusulas no deben confundirse con las cláusulas tipo de protección de datos en el sentido del artículo 46, apartado 2, letras c y d del RGPD, y las partes no podrán invocar las Cláusulas como instrumento de transferencia en virtud del capítulo 5 del RGPD.

9. Asistencia al responsable del tratamiento

1. Teniendo en cuenta la naturaleza del tratamiento, el encargado asistirá al responsable del tratamiento con las medidas técnicas y organizativas adecuadas, en la medida

de lo posible, para el cumplimiento de las obligaciones del responsable del tratamiento de responder a las solicitudes de hacer cumplir los derechos del interesado establecidas en el capítulo 3 del RGPD.

Esto implica que el encargado del tratamiento deberá, en la medida de lo posible, asistir al responsable del tratamiento para que cumpla con:

a. el derecho del interesado a ser informado cuando se recojan datos personales
b. el derecho a ser informado cuando no se hayan obtenido los datos personales del interesado
c. el derecho de acceso del interesado
d. el derecho de rectificación
e. el derecho a la eliminación ('derecho al olvido')
f. el derecho a la limitación del tratamiento
g. la obligación de notificación sobre la rectificación o eliminación de los datos personales o la limitación de su tratamiento
h. el derecho a la portabilidad de los datos
i. el derecho a la oposición
j. el derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la creación de perfiles

2. Además de la obligación del encargado del tratamiento de asistir al responsable del tratamiento en virtud de la cláusula 6.3, el encargado deberá, teniendo en cuenta la naturaleza del tratamiento y la información de que disponga, asistir al responsable del tratamiento para garantizar que cumpla con:

    a. La obligación del responsable del tratamiento de notificar la violación de los datos personales a la autoridad de control competente, la Agencia Danesa de Protección de Datos (Datatilsynet), sin demora injustificada y, cuando sea posible, en un lapso no mayor a las 72 horas de haber tenido conocimiento de ella, a menos que sea improbable que la violación de los datos personales genere un riesgo para los derechos y las libertades de las personas físicas;

    b. la obligación del responsable del tratamiento de comunicar sin demora injustificada la violación de los datos personales al interesado, cuando esta pueda suponer un riesgo alto para los derechos y las libertades de las personas físicas;

    c. la obligación del responsable del tratamiento de llevar a cabo una evaluación del impacto de las operaciones previstas de tratamiento sobre la protección de los datos personales (una evaluación de impacto sobre la protección de los datos personales);

    d. la obligación del responsable del tratamiento de consultar a la autoridad de control competente, la Agencia Danesa de Protección de Datos (Datatilsynet), antes del tratamiento cuando una evaluación del impacto en la protección de datos indique que el tratamiento supondría un riesgo alto en ausencia de medidas adoptadas por el responsable del tratamiento para mitigarlo.

3. Las partes definirán en el Anexo C las medidas técnicas y organizativas adecuadas por las que el encargado del tratamiento debe asistir al responsable del tratamiento, así como el alcance y la extensión de la asistencia requerida. Esto se aplica a las obligaciones previstas en la Cláusula 9.1 y 9.2.

10. Notificación de la violación de datos personales

1. En caso de que se produzca una violación de los datos personales, el encargado del tratamiento deberá notificar al responsable del tratamiento sobre la misma, sin demora injustificada después de haber tenido conocimiento de ella.

2. La notificación del encargado del tratamiento al responsable del tratamiento se realizará, si es posible, dentro de las 24 horas posteriores al momento en que el encargado haya tenido conocimiento de la violación de los datos personales, con el fin de que el responsable del tratamiento cumpla con su obligación de notificar a la autoridad de control competente sobre la violación de los datos personales, véase. Artículo 33 del RGPD.

3. En virtud de la cláusula 9, apartado 2a, el encargado del tratamiento asistirá al responsable del tratamiento a notificar la violación de los datos personales a la autoridad de control competente, lo que significa que el encargado debe asistir en la obtención de la información que se indica a continuación y que, de conformidad con el artículo 33, apartado 3 del RGPD, deberá figurar en la notificación del responsable del tratamiento a la autoridad de control competente:

    a. La naturaleza de los datos personales, incluyendo, cuando sea posible, las categorías y el número aproximado de interesados afectados, así como las categorías y el número aproximado de registros de datos personales afectados;

    b. las probables consecuencias de la violación de los datos personales;

    c. las medidas tomadas o propuestas por el responsable del tratamiento para hacer frente a la violación de los datos personales, incluyendo, cuando corresponda, medidas para mitigar sus posibles efectos adversos.

4. Las partes definirán en el anexo C todos los elementos que debe proporcionar el encargado del tratamiento al asistir al responsable del tratamiento en la notificación de la violación de los datos personales ante la autoridad de control competente.

11. Eliminación y devolución de datos

1. Al finalizar la prestación de servicios de tratamiento de datos personales, el encargado del tratamiento tendrá la obligación de eliminar y/o devolver los datos personales procesados en nombre del responsable y verificar ante el responsable del tratamiento que así lo ha hecho, a menos que la legislación de la Unión o de los Estados Miembros exija la conservación de los datos personales.

12. Auditoría e inspección

1. El encargado del tratamiento pondrá a disposición del responsable del tratamiento toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el artículo 28 y de las Cláusulas, así como también permitirá y contribuirá a las auditorías, incluidas las inspecciones, realizadas por el responsable del tratamiento u otro auditor designado por este.

2. Los procedimientos aplicables a las auditorías del responsable del tratamiento, incluidas las inspecciones, al encargado y subencargado del tratamiento se indican en el anexo C.7 y C.8.

3. El encargado del tratamiento estará obligado a proporcionar a las autoridades de control, que en virtud de la legislación vigente tiene acceso a las instalaciones del responsable y del encargado del tratamiento, o a los representantes que actúen en

nombre de dichas autoridades de control, el acceso a las instalaciones físicas del encargado cuando se le presentase la identificación apropiada.

13. Acuerdo de las partes sobre otras condiciones

1. Las partes pueden acordar otras cláusulas relativas a la prestación del servicio de tratamiento de los datos personales especificando, por ejemplo, la responsabilidad, siempre que no contradigan de forma directa o indirecta las Cláusulas ni perjudiquen los derechos o libertades fundamentales del interesado y la protección que otorga el RGPD.

14. Inicio y finalización

1. Las Cláusulas entrarán en vigor en la fecha de la firma del acuerdo de licencia por ambas partes.

2. Ambas partes tendrán derecho a exigir la renegociación de las Cláusulas si los cambios en la legislación o la falta de conveniencia de las Cláusulas dieran lugar a dicha renegociación.

3. Las Cláusulas regirán mientras dure la prestación de los servicios de tratamiento de los datos personales. Mientras dure la prestación de servicios de tratamiento de datos personales, no será posible rescindir las Cláusulas a menos que las partes hayan acordado otras Cláusulas que rijan la prestación de servicios de tratamiento de datos personales.

4. Si se pone fin a la prestación de servicios de tratamiento de los datos personales, y estos son eliminados o devueltos al responsable del tratamiento según lo establecido en la Cláusula 11.1 y Anexo C.4, las Cláusulas podrán rescindirse mediante notificación por escrito de cualquiera de las partes.

15. Contacto

1. El responsable del tratamiento puede contactar al encargado del tratamiento en: dataprivacy@samesystem.com para todas las consultas generales sobre estas Cláusulas y en caso de violación de datos.

Anexo A) Información sobre el tratamiento

A.1. El fin del tratamiento de datos personales por parte del encargado en nombre del responsable del tratamiento es:

Que el responsable del tratamiento pueda aplicar el sistema de gestión de personal en línea de SameSystem, con el objetivo de recopilar y procesar información sobre sus empleados y gestionar su plantilla.

A.2. El tratamiento de los datos personales por parte del encargado del tratamiento en nombre del responsable del tratamiento se refiere principalmente a (la naturaleza del tratamiento):

El encargado del tratamiento pone a SameSystem a disposición del responsable del tratamiento y en nombre de este almacena datos personales sobre los empleados del responsable en los servidores del encargado del tratamiento y de los subencargados aprobados.

A.3. El tratamiento incluye los siguientes tipos de datos personales sobre los interesados:

- Nombre
- Fecha de nacimiento
- Número de la seguridad social/número de seguridad nacional
- Dirección de correo electrónico
- Número de teléfono
- Domicilio
- Salario/pensión
- Nómina y número de empleado
- Posición laboral
- Horas de trabajo
- Departamento
- Correspondencia entre los interesados
- Ausencias y permisos (incluídas las licencias por paternidad y ausencias debido a vacaciones, enfermedad, excluidos los certificados médicos)
- Advertencias/despidos
- Beneficios
- Otras funciones/responsabilidades laborales

Todos los datos personales a los que tenga acceso el encargado del tratamiento deben ser tratados de manera confidencial.

A.4. El tratamiento incluye las siguientes categorías de interesados:

- Empleados del responsable del tratamiento.

A.5. El tratamiento de los datos personales por parte del encargado del tratamiento en nombre del responsable del tratamiento se puede realizar a partir de la entrada en vigor de las Cláusulas. El tratamiento tiene la siguiente duración:

Las Cláusulas permanecerán en vigor hasta la finalización del acuerdo de licencia y se extinguirán de acuerdo con la cláusula 14 que figura anteriormente.

Anexo B) Subencargados autorizados

B.1. Subencargados aprobados

A partir de la entrada en vigor de las Cláusulas, el responsable del tratamiento autoriza la contratación de los siguientes subencargados:

NOMBRE	PAÍS DE ALOJAMIENTO	DIRECCIÓN INCLUIDO EL PAÍS	DESCRIPCIÓN DEL TRATAMIENTO
SameSystem UAB, LT100004691219	Sin almacenamiento de datos	Didžioji g. 25, LT-01130, Vilnius, Lituania	Desarrollo y mejora del sistema informático. Ayuda técnica, si es necesaria.
Hetzner Online GmbH, DE812871812	Alemania (sede principal) y Finlandia (sede de respaldo)	Industrie str. 25, 91710 Gunzenhausen, Alemania	El almacenamiento de todos los datos en el sistema, incluidos los datos personales.
Scaleway SAS	Francia	8 rue de la Ville l'Evêque, 75008 Paris, France	Almacenamiento de datos en Francia. Esto afecta principalmente a los datos de copia de seguridad.
Grupo Link Mobility	Noruega	Langkaia 1 – Havnelageret, 0150, Oslo, Noruega	Envío de SMS. (No se tratan datos en Estados Unidos)
SMTP.DK ApS	Dinamarca	Refshalevej 163A, 1. Tv 1432 København K, Dinamarca	Envío de correos electrónicos.
E-Signatur Danmark A/S CVR. 38491687	Irlanda	Lersø Park Alle 107, 2100 København Ø. Dinamarca	Firmas digitales
Sendbird, Inc	Alemania	400 1st Ave San Mateo, California 94401 Estados Unidos	Funciones de chat y mensajería interna dentro de la solución SameSystem (chat entre los usuarios). Solo se procesan el 'nombre para mostrar' y el chat o mensajes. **Nota**: Este es un servicio **opcional**, que el cliente puede elegir que SameSystem active para él.

El responsable del tratamiento autorizará, en el momento de entrada en vigor de las Cláusulas, el uso de los subencargados antes mencionados para el tratamiento descrito para dicha parte. El encargado del tratamiento no tendrá derecho, sin la autorización explícita y por es-

crito del responsable del tratamiento, a contratar a un subencargado para un tratamiento 'diferente' al que ha sido acordado, o a disponer de otro subencargado para que realice el tratamiento descrito.

B.2. Aviso previo para la autorización de los subencargados

El encargado del tratamiento informará al responsable del tratamiento de cualquier modificación a la lista de subencargados con un mínimo de 30 días de anticipación, y permitirá al responsable del tratamiento oponerse al cambio en la lista de subencargados. En caso de que el responsable del tratamiento no haya expresado su oposición al cambio de subencargado o a la contratación de un nuevo subencargado dentro del plazo establecido, el subencargado se considerará aceptado.

Si la modificación en la lista de subencargados incluye la adición de un subencargado en un tercer país, el responsable del tratamiento debe ser notificado como se acuerda en el anexo C, cláusula C.6.

Anexo C) Instrucciones relativas a la utilización de datos personales

C.1. El tema de las/instrucciones para el tratamiento

El tratamiento de los datos personales por parte del encargado del tratamiento en nombre del responsable del tratamiento será llevado a cabo por el encargado, que realizará lo siguiente:

El encargado del tratamiento pone SameSystem a disposición del responsable del tratamiento según lo descrito en el acuerdo de licencia y en las condiciones generales de la licencia y, con el fin de cumplir con el acuerdo de licencia, almacenará en nombre del responsable del tratamiento los datos personales de los empleados de este último en los servidores del encargado del tratamiento y en los subencargados relevantes según se enumeran, se describen y son aprobados por el responsable del tratamiento en el Anexo B, B1.

El encargado del tratamiento tiene instrucciones de procesar los datos personales únicamente para este fin y no tiene derecho a tratar o utilizar los datos personales del responsable del tratamiento para ningún otro propósito.

C.2. Seguridad del tratamiento

Esta sección describe los requisitos mínimos de seguridad para el nivel de seguridad interna y los controles del encargado del tratamiento.

C.2.1.1 Organización de la seguridad de la información (A.5 Política de seguridad y A.6 Funciones y responsabilidad)

El encargado del tratamiento debe tener una política de seguridad documentada que aborde la protección de la información para todo el personal empleado por el encargado del tratamiento. La política de seguridad debe revisarse y actualizarse al menos una vez al año. Debe existir una política sobre el tratamiento de los datos personales; puede estar incluida en la política de seguridad de la información. Debe disponer en todo momento de un inventario de políticas y procedimientos, y este debe recibir mantenimiento con una frecuencia definida por el encargado del tratamiento para reflejar las obligaciones acordadas en las Cláusulas.

La función de seguridad de la información debe ser responsable de las iniciativas de seguridad dentro de la organización del encargado del tratamiento. Una persona designada debe ser responsable de los servicios de seguridad de la información proporcionados al responsable del tratamiento.

El encargado del tratamiento debe disponer de las correspondientes evaluaciones actualizadas de los riesgos para la seguridad de la información, que, previa solicitud, deben ponerse a disposición del responsable del tratamiento antes de que se presten o modifiquen los servicios.

El encargado del tratamiento debe mantener evaluaciones de riesgo sobre el acceso a los datos, sistemas y redes por parte de terceros.

Las funciones y responsabilidades relacionadas con la política de seguridad de la información, incluido el tratamiento de datos personales, deben definirse y describirse con claridad.

C.2.1.2 Concientización sobre la seguridad (A.7 Seguridad de los Recursos Humanos)

El encargado del tratamiento debe implementar un programa de concientización sobre la seguridad de la información y la protección de los datos para capacitar a todos los empleados que tengan acceso o manejen los datos del responsable del tratamiento.

C.2.1.3 Gestión de activos y dispositivos (A.8 Gestión de activos)

La organización debe contar con un registro de los recursos informáticos utilizados para el tratamiento de los datos personales en nombre del responsable del tratamiento. El mismo debe ser mantenido por un recurso específico, que también revisa y actualiza la lista periódicamente, al menos una vez al año.

Todos los dispositivos que sean relevantes en el manejo y/o tratamiento de los datos del encargado del tratamiento, incluidas las llaves USB y otros dispositivos móviles, deben estar protegidos, por ejemplo, mediante el cifrado de disco duro, contraseñas fuertes utilizadas para proteger contra el acceso no autorizado a los datos personales y la limitación del acceso para incluir únicamente a los empleados con fines específicos relacionados con el trabajo. "Las contraseñas deben almacenarse en forma de hash." El inicio de sesión se debe bloquear automáticamente después de 5 intentos fallidos como protección contra el acceso no autorizado a los datos personales.

Si la información personal puede tratarse en los dispositivos propiedad de los empleados (BYOD, por su nombre en inglés) del encargado del tratamiento, estos dispositivos deben contar con una seguridad adecuada, incluyendo cifrado, contraseñas apropiadas forzadas y la limitación del acceso a los empleados con fines específicos relacionados con el trabajo, por ejemplo, con tecnologías de sandboxing. Las políticas de BYOD, las directrices y las políticas de protección de datos deben ponerse a disposición, previa solicitud, del responsable del tratamiento; esto también incluye adoptar una herramienta de Gestión de Dispositivos Móviles (MDM) para hacer cumplir lo anterior.

El encargado del tratamiento debe garantizar el control de todos los activos utilizados para prestar los servicios al responsable del tratamiento, lo que garantiza que todos los datos de este último se sobreescriben de manera segura mediante un software especializado antes de la retirada del hardware o su reutilización para otros fines.

Los soportes externos que se utilicen, incluidas las llaves USB, las tabletas, teléfonos inteligentes, etc. deben estar cifrados y borrados de manera segura o destruidos cuando se retiren como protección contra el acceso no autorizado a los datos personales.

Los discos y los soportes extraíbles deben almacenarse y protegerse contra el acceso no autorizado durante la reparación, el mantenimiento y cuando son transportados, y deben manipularse de acuerdo con todos los requisitos de seguridad.

C.2.1.4 Gestión del acceso (A.9 Control del acceso)
El encargado del tratamiento debe tener claramente definidas las funciones y responsabilidades de los empleados. Antes de la contratación, se debe llevar a cabo una "selección pertinente" [que puede incluir la evaluación de lo siguiente: comprobación de antecedentes, antecedentes penales, empleador anterior, etc.] y se deben aplicar adecuadamente las condiciones de empleo.

El encargado del tratamiento debe implementar procedimientos de administración de usuarios, que definen sus funciones y privilegios, y si el acceso ha sido otorgado, modificado o cancelado, lo que aborda una segregación adecuada de las tareas, y lo que define los requisitos y mecanismos de registro y monitoreo.

El acceso privilegiado a los datos, las aplicaciones y la infraestructura debe estar limitado a las personas con un propósito comercial específico y documentado. Los derechos de acceso y el uso autorizado de los datos personales deben describirse por escrito para las funciones laborales relevantes.

El encargado del tratamiento debe garantizar un control documentado, eficiente y periodico de los derechos asignados a todos los tipos de cuentas de usuarios en todos los sistemas que dan apoyo a los servicios del responsable del tratamiento. La revisión de control se debe actualizar como mínimo una vez cada doce meses para las cuentas de usuarios finales y como mínimo cada seis meses para las cuentas con privilegios. Se deberá desactivar las credenciales de los usuarios que renuncien o sean dados de baja inmediatamente después de su último día de trabajo.

El encargado del tratamiento debe apoyar al responsable del tratamiento en la revisión de las cuentas de este último. A petición del responsable del tratamiento, el encargado del tratamiento debe proporcionar un resumen de los derechos de acceso de cada empleado a los datos y sistemas del responsable.

Se debe asignar una identificación de usuario única a cada uno de los empleados y se prohibe la reemisión de identificaciones de usuarios desactivadas o caducadas.

Los derechos de acceso se deben implementar siguiendo el enfoque del "mínimo privilegio".

Debe exigirse la autenticación de dos factores para el acceso privilegiado a los datos, las aplicaciones y la infraestructura.

El acceso remoto a los datos, las aplicaciones y la infraestructura debe requerir una autorización de doble factor.

C.2.1.5 Seguridad física (A.11 Seguridad física y ambiental)
Las salas de servidores, centros de datos y zonas de oficinas desde las que se puede acceder potencialmente a los datos del responsable del tratamiento deben estar protegidos contra el acceso no autorizado.

En todos estos lugares debe implementarse el control del acceso físico. Debe prohibirse el acceso no autorizado mediante la vigilancia las 24 horas, los 7 días de la semana y la limitación del acceso con un registro de auditoría de acceso electrónico. Debe establecerse una identificación clara a través de los medios adecuados, por ejemplo, tarjetas de identificación para todo el personal y los visitantes que accedan a las instalaciones, según corresponda.

Las instalaciones deben estar equipadas con las instalaciones técnicas correspondientes para garantizar la disponibilidad de los servicios.

C.2.1.6 Seguridad en el lugar (A.11 Seguridad física y ambiental)
Los documentos físicos deben manejarse de manera segura y protegerse desde la impresión, el almacenamiento seguro hasta la destrucción física, por ejemplo, mediante el uso de impresión "FollowMe" e impresoras ubicadas en un lugar seguro de acceso limitado. Los archivadores deben colocarse en un lugar seguro con acceso limitado o en un almacén seguro. Los armarios deben estar protegidos según la clasificación de lo que se almacena en ellos.

Debe implementarse un control de acceso físico para proteger todos los tipos de datos personales en todos los soportes dentro de cada lugar, desde oficinas y salas de servidores hasta las impresoras y faxes que podrían producir impresiones que contengan los datos personales del responsable del tratamiento.

Esto incluye la protección contra los riesgos de que personas no autorizadas miren las pantallas de los ordenadores, personas que lean documentos dejados en los escritorios, personal de limpieza con acceso fuera del horario de trabajo, por ejemplo, datos personales sensibles guardados bajo llave en armarios, etc. Debe utilizarse una 'política de escritorio limpio' para prevenir lo anterior.

C.2.1.7 Actualización, parcheado y control de cambios (A.12 Operación)
El encargado del tratamiento debe garantizar que los parches del sistema y del software se completen según las recomendaciones del proveedor en todos los sistemas e infraestructuras que pueden proporcionar servicios al responsable del tratamiento, incluidas las estaciones de trabajo internas, aplicaciones y servidores.

El encargado del tratamiento debe completar las actualizaciones de seguridad. Debe revisarse e instalarse los parches de seguridad fundamentales e importantes lo antes posible.

C.2.1.8 Relaciones con los proveedores (A.15 Relaciones con los subencargados)

Antes de que un subencargado realice el tratamiento de los datos personales, deben establecerse directrices y procedimientos formales que incluyan las medidas contractuales relevantes que cubran los presentes criterios para el tratamiento de datos personales. En caso de que el responsable del tratamiento lo solicite, debe ponerse a su disposición, en un plazo razonable y sin demoras injustificadas, la documentación que demuestre que el subencargado cumple con estas Cláusulas y/o con el RGPD y/o con la legislación pertinente del Estado Miembro. Estas directrices, procedimientos y medidas contractuales establecerán, como mínimo, el mismo nivel de protección y seguridad de los datos personales que se indica en estas Cláusulas.

C.2.1.9 Protección contra el malware (A.12 Seguridad de las operaciones)
Debe instalarse y mantenerse una protección actualizada contra el malware en todos los sistemas y hardware del encargado del tratamiento que se utilicen para el tratamiento de datos personales en nombre del responsable del tratamiento o que estén conectados con los sistemas o hardware administrados por el encargado del tratamiento.

C.2.1.10 Copia de seguridad (A.12 Seguridad de las operaciones)
El encargado del tratamiento debe contar con una política de copia de seguridad documentada y llevar a cabo una copia de seguridad de los sistemas y datos del responsable del tratamiento. Los requisitos de conservación y eliminación de los datos deben definirse y tratarse de acuerdo con las políticas y los procedimientos.

El encargado del tratamiento debe implementar procedimientos para verificar las copias de seguridad restableciendo satisfactoriamente los datos, el software y los sistemas respaldados al menos cada 6 meses. La documentación debe estar disponible cuando se solicite y debe incluirse en los informes/KPI.

Las copias de seguridad deben estar protegidas del acceso no autorizado.

Las copias de seguridad deben estar cifradas y almacenarse de manera segura.

C.2.1.11 Registro y supervisión (A.12 Seguridad de las operaciones)
Se debe registrar todo acceso a los datos personales. El registro de acceso debe incluir la fecha y hora en que se produjo, la identificación del usuario y el tipo de acceso (lectura, edición, eliminación, y en los datos sensibles también la visualización y búsqueda de datos, etc.).

El registro de seguridad debe estar habilitado en todos los equipos de la red, los servidores y en todas las aplicaciones incluidas las bases de datos y los administradores de sistemas informáticos; los archivos de registro deben tener una marca de tiempo y estar adecuadamente protegidos contra la manipulación y el acceso no autorizado. Los relojes deben estar sincronizados con una única fuente de horario. Los registros se deben supervisar, por ejemplo, estableciendo reglas para las alarmas si los registros muestran anomalías antes las que el encargado del tratamiento debe reaccionar.

Por lo tanto, debe establecerse un sistema centralizado de recogida y revisión de los registros de seguridad.

Los registros de acceso a los datos personales y el uso de dichos datos deben ser supervisados y estar disponibles para su revisión con el fin de detectar el acceso no autorizado a los datos personales. Se debe documentar cuándo y con qué frecuencia se revisan los archivos de registro y quién ha realizado el control. La documentación debe estar disponible cuando se solicite.

Los intentos fallidos de inicio de sesión deben registrarse y guardarse por 6 meses para detectar el acceso no autorizado a los datos personales.

C.2.1.12 Seguridad de la red (A.13 Seguridad de las comunicaciones)

El encargado del tratamiento debe mantener la seguridad de la red utilizando equipos disponibles en el mercado y técnicas estándar de la industria, incluyendo cortafuegos y sistemas de detección de intrusos.

La infraestructura debe estar segmentada como mínimo para separar los sistemas de producción de los entornos de prueba y desarrollo.

Todos los datos personales transmitidos por el encargado del tratamiento deben estar cifrados mientras están en tránsito y en reposo.

C.2.1.13 Gestión de incidentes de seguridad (A.16 Gestión de incidentes)
El encargado del tratamiento debe implementar procedimientos para la detección, análisis y manejo rápido y eficaz de los incidentes de seguridad.

Todos los incidentes de seguridad y violaciones de la seguridad relacionadas con los servicios proporcionados al responsable del tratamiento deben informarse a este sin demora injustificada.

El encargado del tratamiento debe implementar los requisitos de notificación señalados en el RGPD y proporcionar la información necesaria al responsable del tratamiento dentro de las 24 horas.

C.2.1.14 Recuperación ante desastres y continuidad del negocio (A. 17 Aspectos de la seguridad de la información en la gestión de la continuidad del negocio)
El encargado del tratamiento debe implementar un plan de recuperación ante desastres documentado y probado, así como una estrategia de continuidad del negocio que cubra los sistemas del responsable del tratamiento siguiendo un nivel de servicio acordado.

Los planes de recuperación de desastres y las estrategias de continuidad del negocio deben probarse y actualizarse periódicamente, y al menos una vez al año, para garantizar que estén al día y que sean eficaces. La documentación debe estar disponible cuando se solicite.

C.2.1.15 Tratamiento de datos (C.7.3.8)
El encargado del tratamiento debe poder proporcionar al responsable del tratamiento una copia de toda la información procesada por el encargado sobre un interesado determinado, previa solicitud, de forma estructurada, de uso común y legible por máquina

C.2.2 Requisitos de seguridad específicos de la solución

C.2.2.1 Servicios en la nube
El encargado del tratamiento realizará un análisis de riesgos de los supresores pertinentes basados en la nube. Se deberá proporcionar al responsable del tratamiento los acuerdos de los subencargados con eventuales proveedores en la nube que formen parte de la solución, previa solicitud.

C.2.2.2 Seguridad del ciclo de vida de las aplicaciones (A.14 Adquisición, desarrollo y mantenimiento de los sistemas)
Durante el ciclo de vida del desarrollo deben seguirse las mejores prácticas, las prácticas de desarrollo seguro más avanzadas y reconocidas, los marcos o las normas, lo que significa que el encargado del tratamiento debe implementar los principios de protección de datos por diseño y por defecto en todas las fases del ciclo de vida del tratamiento de datos y del sistema. Esto implica que no solo se recoja la información pertinente, proporcional y necesaria, incluyendo el uso, la divulgación, la retención, la transmisión y la eliminación de la información sobre los individuos para la aplicación que procesa los datos.

Los datos personales no deben utilizarse en los entornos de desarrollo o de prueba sin ser anonimizados, pseudonimizados, codificados o enmascarados antes de su uso.

El desarrollo del sistema debe producirse en entornos de desarrollo especializados, aislados de los sistemas de producción y prueba, y debe estar protegido contra el acceso no autorizado.

El código fuente debe estar protegido contra el acceso y el uso no autorizados.

El encargado del tratamiento debe llevar a cabo revisiones de seguridad, comprobaciones de vulnerabilidad y pruebas de penetración de todo el código y las aplicaciones desarrolladas para el responsable del tratamiento antes de su publicación. Se deben realizar y documentar pruebas periódicas PEN en las aplicaciones orientadas a la web.

C.3. Asistencia al responsable del tratamiento

El encargado del tratamiento deberá, en la medida de lo posible -dentro del ámbito y del alcance de la asistencia especificada a continuación- colaborar con el responsable del tratamiento de acuerdo con la Cláusula 9.1 y 9.2 implementando las siguientes medidas técnicas y organizativas:

El encargado del tratamiento tiene el deber de asistir al responsable del tratamiento en el cumplimiento de sus obligaciones establecidas en el presente acuerdo sin demora injustificada.

C.4. Periodo de almacenamiento/procedimientos de eliminación

La autorización del encargado del tratamiento para procesar datos personales en nombre del responsable del tratamiento finaliza cuando se extinguen las Cláusulas o el acuerdo de licencia.

Tras la extinción de las Cláusulas, el encargado del tratamiento y sus subencargados devolverán y/o eliminarán todos los datos personales que el encargado haya tratado en virtud de las Cláusulas, de acuerdo con la Cláusula 14 que figura anteriormente. El responsable del tratamiento puede exigir la documentación.

No obstante, se permite al encargado del tratamiento continuar con el tratamiento de los datos personales hasta un mes después de la finalización de las Cláusulas, si la extensión de los datos requiere una mayor cantidad de trabajo para el encargado. El encargado del procesamiento tiene derecho, en el mismo periodo, a que los datos personales sean parte del procedimiento normal de copia de seguridad. El tratamiento de los datos personales por parte del encargado del tratamiento durante este periodo continuará con las mismas instrucciones descritas en las Cláusulas.

C.5. Lugar de tratamiento

Las ubicaciones del encargado del tratamiento y de los subencargados se enumeran en el Anexo B, B.1

El tratamiento de los datos personales en virtud de las Cláusulas no puede llevarse a cabo en otros sitios diferentes a los enumerados en el Anexo B, B.1. Otros lugares o sitios nuevos de tratamiento requerirán una notificación previa por parte del encargado del tratamiento según lo establecido en el Anexo B, B2 en las Cláusulas que indica que la contratación de eventuales subencargados nuevos (y por lo tanto, eventualmente nuevos lugares de tratamiento) debe ser notificada al responsable del tratamiento al menos 60 días antes de su uso previsto.

C.6. Instrucciones sobre la transferencia de datos personales a terceros países

C.6.1 El encargado del tratamiento puede transferir los datos a un subencargado aprobado de acuerdo con la cláusula 7.3 del presente acuerdo.

C.6.2 El encargado del tratamiento garantizará un fundamento legal para la transferencia de acuerdo con el Capítulo 5 del RGPD, sin necesidad de la firma del responsable del tratamiento. En estos casos, el encargado del tratamiento es responsable de garantizar la legalidad del fundamento de la transferencia.

C.6.3 En caso de transferencia de datos a un tercer país, el responsable del tratamiento debe ser informado con al menos 90 días de antelación a la transferencia. Si el responsable del tratamiento no se opone a la transferencia dentro de este plazo, la transferencia se aprobará en virtud de la cláusula 7.3 del presente acuerdo.

Si el responsable del tratamiento no proporciona instrucciones documentadas relativas a la transferencia de datos personales a un tercer país según se indica en estas Cláusulas, el encargado del tratamiento no estará autorizado, en el marco de las Cláusulas, a realizar dicha transferencia.

C.7. Procedimientos para las auditorías del responsable del tratamiento, incluidas las inspecciones, del tratamiento de los datos personales que realiza el encargado del tratamiento

El encargado del tratamiento obtendrá una vez al año, a expensas del propio encargado, un informe de auditoría o de certificación de un tercero independiente sobre el cumplimiento por parte del encargado del tratamiento del RGPD, de las disposiciones de protección de datos de la UE o de los Estados Miembros y de las Cláusulas.

Las partes han acordado que se puede utilizar el siguiente tipo de auditoría y certificación en cumplimiento de las Cláusulas:

ISAE3000

El informe o la certificación aprobados se enviarán al responsable del tratamiento, previa solicitud, sin demora injustificada para acreditar el cumplimiento de los criterios establecidos en las presentes Cláusulas. El informe o certificación aprobado también estará disponible en www.samesystem.com. El responsable del tratamiento podrá impugnar el alcance y/o la metodología del informe y, en tal caso, podrá solicitar una nueva auditoría/inspección con un alcance revisado y/o una metodología diferente. El encargado del tratamiento tiene derecho a cobrar una tarifa horaria razonable por el servicio regulado en el Apéndice D de estas Cláusulas si el responsable del fichero solicita otras auditorías y/o certificaciones distintas de las indicadas en el apartado anterior.

Sobre la base de los resultados de dicha auditoría/inspección, el responsable del tratamiento podrá solicitar que se tomen medidas adicionales para garantizar el cumplimiento de lo establecido en el RGPD, las disposiciones de protección de datos aplicables de la UE o de los Estados Miembros y las Cláusulas.

El responsable del tratamiento o su representante tendrá además acceso a inspeccionar, incluso físicamente, los lugares donde se lleva a cabo el tratamiento de los datos personales por el encargado del tratamiento, entre ellos las instalaciones físicas y los sistemas utilizados para y en conexión con el tratamiento en nombre del responsable del tratamiento. Dicha inspección se llevará a cabo cuando el responsable del tratamiento lo considere necesario y cuando tenga una finalidad concreta y relevante.

C.8. Procedimientos para las auditorías, incluidas las inspecciones, del procesamiento de datos personales llevado a cabo por los subencargados

La auditoría o certificación acordada en la cláusula del anexo C.7 incluirá a los subencargados utilizados en la prestación del servicio dentro su alcance.

Si los subencargados no forman parte del alcance de la auditoría o certificación acordada en el punto C.7,
el encargado del tratamiento obtendrá una vez al año, a expensas del propio encargado, una auditoría o certificación de un tercero independiente sobre el cumplimiento por parte del subencargado con lo establecido en el RGPD, las disposiciones aplicables de protección de datos de la UE o de los Estados Miembros y de las Cláusulas, o realizará la inspección pertinente del subencargado de acuerdo con las normas anteriores o similares, como se indica en la cláusula C.7.

El informe o la certificación aprobados se enviarán al responsable del tratamiento, previa solicitud, sin demora injustificada, para acreditar el cumplimiento de los criterios establecidos en las presentes Cláusulas. El responsable del tratamiento podrá impugnar el alcance y/o la metodología del informe y podrá, en tales casos, solicitar una nueva auditoría o inspección con un alcance revisado y/o una metodología diferente. El encargado del tratamiento tiene derecho a cobrar una tarifa horaria razonable por el servicio si el responsable del tratamiento exige otras auditorías y/o certificaciones diferentes a las establecidas anteriormente.

Sobre la base de los resultados de dicha auditoría/inspección, el responsable del tratamiento podrá solicitar que se tomen medidas adicionales para garantizar el cumplimiento de lo establecido en el RGPD, las disposiciones de protección de datos aplicables de la UE o de los Estados Miembros y las Cláusulas.

El encargado del tratamiento o su representante tendrá además acceso a inspeccionar, incluso físicamente, los lugares donde se lleva a cabo el tratamiento de los datos personales por parte del subencargado, entre ellos las instalaciones físicas y los sistemas utilizados para y en conexión con el tratamiento. Dicha inspección se realizará cuando el encargado del tratamiento (o el responsable del tratamiento) lo considere necesario y cuando tenga una finalidad concreta y relevante.

La documentación de dichas inspecciones deben presentarse sin demora al responsable del tratamiento a fines informativos. El responsable del tratamiento podrá impugnar el alcance y/o la metodología del informe y podrá, en tales casos, solicitar una nueva inspección con un alcance revisado y/o una metodología diferente cuando tenga una finalidad concreta y relevante.

El responsable del tratamiento podrá, en caso necesario, optar por iniciar y participar de la inspección física del subencargado. Esto puede aplicarse si el responsable del tratamiento considera que la supervisión del subencargado por parte del encargado del tratamiento no ha proporcionado al responsable la documentación suficiente para determinar que el tratamiento realizado por el subencargado cumple con las Cláusulas.

La participación del responsable del tratamiento en una inspección del subencargado no alterará el hecho de que, en adelante, el encargado del tratamiento continúe siendo plenamente responsable del cumplimiento por parte del subencargado del RGPD de las disposiciones de protección de datos aplicables de la UE o de los Estados Miembros y de las Cláusulas.

Los costos del encargado del tratamiento y del subencargado relacionados con la supervisión/inspección física en las instalaciones del subencargado no afectarán al responsable del tratamiento, independientemente de que el responsable haya iniciado y participado de dicha inspección cuando esta tenga un propósito concreto y relevante.

Anexo D) Las condiciones de acuerdo de las partes sobre otros temas

En cuanto a los puntos 9.2 y C.7

En la medida en que el responsable del tratamiento solicite la asistencia del encargado del tratamiento en los servicios descritos en la cláusula 9.2 (c) y (d), y en caso de que el responsable del tratamiento exija otras auditorías o/y certificaciones que las indicadas anteriormente en el Anexo C, cláusula C.7, el responsable del tratamiento está obligado a remunerar al encargado del tratamiento por el tiempo empleado en ello según las tarifas horarias utilizadas por el encargado del tratamiento en ese momento.

Cambios en el acuerdo de tratamiento de datos

Entre las partes se aplica siempre la última versión del acuerdo de tratamiento de datos.

El responsable del tratamiento de datos se reserva el derecho a introducir continuamente cambios y aclaraciones en el acuerdo. Estos cambios suelen ser el resultado de nuevas recomendaciones de, por ejemplo, la Autoridad de Protección de Datos o la Comisión de la UE, así como de cambios en la práctica y la legislación en la materia.

Por lo tanto, se recomienda al responsable del tratamiento que se inscriba para recibir notificaciones cuando se produzcan cambios en el acuerdo.

Tras recibir la notificación de un cambio, el responsable del tratamiento dispone de 14 días laborables para oponerse si el cambio no puede aceptarse razonablemente.

Esta disposición no se aplica a los cambios en el uso de subencargados del tratamiento de datos, que se regulan en la sección 7 del acuerdo.