

Anexo sobre el tratamiento de datos subcontratado (en virtud del artículo 28 del RGPD) relativo al contrato n.º

Contratista (nombre, dirección, país):

Contenido

- Cláusulas de 1 a 11
- [Apéndice I. Descripción del tratamiento o tratamientos](#)
- [Apéndice II. Lista de subcontratistas](#)
- [Apéndice III. Medidas técnicas y organizativas](#)

Cláusula 1. Finalidad y ámbito de aplicación

- a) La finalidad del presente Anexo sobre el tratamiento de datos subcontratado (en lo sucesivo, “pliego de cláusulas”) es garantizar que se cumpla el artículo 28, apartados 3 y 4, del 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**).
- b) El comitente, como responsable del tratamiento, y el contratista, como encargado del tratamiento, (en lo sucesivo, “las partes”) han dado su consentimiento a vincularse por el presente pliego de cláusulas a fin de garantizar el cumplimiento del artículo 28, apartados 3 y 4, del Reglamento (UE) 2016/679.
- c) El presente pliego de cláusulas se aplica al tratamiento de datos personales especificado en el apéndice I.
- d) Los apéndices I a III forman parte del pliego.
- e) El presente pliego de cláusulas se entiende sin perjuicio de las obligaciones a las que esté sujeto el comitente en virtud del Reglamento (UE) 2016/679.
- f) El presente pliego de cláusulas no garantiza por sí mismo el cumplimiento de las obligaciones relativas a las transferencias internacionales contempladas en el capítulo V del Reglamento (UE) 2016/679. Cuando una transferencia de datos personales del comitente al contratista implique la transferencia a un tercer país, se requerirá un fundamento jurídico para dicha transferencia de datos. En ausencia de una decisión de adecuación de conformidad con el artículo 45 del Reglamento (UE) 2016/679 o de garantías adecuadas de conformidad con el artículo 46 del Reglamento (UE) 2016/679, y si tampoco es aplicable ninguna de las excepciones para situaciones específicas contempladas en el artículo 49 del Reglamento (UE) 2016/679, se celebrará un acuerdo vinculante entre el comitente y el contratista para establecer un fundamento jurídico. Tal acuerdo consistirá en la adopción de cláusulas tipo de protección de datos de conformidad con el artículo 46, apartado 1, y el artículo 46, apartado 2, letra c), del Reglamento (UE) 2016/679.

Cláusula 2. Invariabilidad del pliego de cláusulas

Las partes se comprometen a no modificar el pliego de cláusulas, excepto para añadir o actualizar información en los apéndices. Los complementos o las actualizaciones de la información de los apéndices no requerirán un complemento al contrato por escrito y se podrán acordar en forma de texto.

Cláusula 3. Interpretación

- a) Cuando en el presente pliego de cláusulas se utilizan términos definidos en el Reglamento (UE) 2016/679, se entiende que tienen el mismo significado que en el Reglamento correspondiente.
- b) El presente pliego de cláusulas deberá leerse e interpretarse con arreglo a las disposiciones del Reglamento (UE) 2016/679.
- c) No se podrán realizar interpretaciones del presente pliego de cláusulas que entren en conflicto con los derechos y obligaciones establecidos en el Reglamento (UE) 2016/679 y/o que perjudiquen los derechos o libertades fundamentales de las personas interesadas.

Cláusula 4. Jerarquía

En caso de contradicción entre el presente pliego de cláusulas y las disposiciones de acuerdos conexos entre las partes que estuvieren en vigor en el momento en que se pactare o comenzare a aplicar el presente pliego de cláusulas, prevalecerá el presente pliego de cláusulas.

Cláusula 5. Descripción del tratamiento o tratamientos

En el apéndice I se especifican los pormenores de las operaciones de tratamiento y, en particular, las categorías de datos personales y los fines para los que se tratan los datos personales por cuenta del comitente.

Cláusula 6. Obligaciones de las partes

6.1 Instrucciones

- a) El contratista tratará los datos personales únicamente siguiendo instrucciones documentadas del comitente, salvo que esté obligado al tratamiento en virtud del Derecho de la Unión o de los Estados miembros que se aplique al contratista. En tal caso, el contratista informará al comitente de esa exigencia legal previamente al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público. El comitente también podrá dar instrucciones ulteriores en cualquier momento del período de tratamiento de los datos personales. Una instrucción es una orden escrita, electrónica u oral del comitente referida a un modo específico del contratista de procesar datos. Dichas órdenes deberán estar documentadas. Las instrucciones se definirán primero en los términos de referencia y el comitente podrá modificarlas, complementarlas o sustituirlas posteriormente de forma documentada mediante una instrucción individual.

- b) El contratista informará inmediatamente al comitente si las instrucciones dadas por el comitente infringen, a juicio del contratista, el Reglamento (UE) 2016/679 o las disposiciones aplicables del Derecho de la Unión o de los Estados miembros en materia de protección de datos.
- c) El comitente podrá exigir en cualquier momento la entrega, rectificación, adaptación, supresión o limitación del tratamiento de los datos.
- d) El contratista solo podrá proporcionar información a terceros o a la persona interesada previa aprobación expresa por parte del comitente. Dicha aprobación deberá ser documentada por el contratista.

6.2 Limitación de la finalidad

El contratista tratará los datos personales únicamente para los fines específicos del tratamiento indicados en el apéndice I, salvo cuando siga instrucciones adicionales del comitente.

6.3 Duración del tratamiento de datos personales

El tratamiento por parte del contratista solo se realizará durante el período especificado en el apéndice I.

6.4 Seguridad del tratamiento

- a) El contratista aplicará, como mínimo, las medidas técnicas y organizativas especificadas en el apéndice III para garantizar la seguridad de los datos personales. Una de estas medidas podrá consistir en la protección contra violaciones de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales, o la comunicación o acceso no autorizados a dichos datos (en lo sucesivo, “violación de la seguridad de los datos personales”). A la hora de determinar un nivel adecuado de seguridad, las partes tendrán debidamente en cuenta el estado de la técnica, los costos de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, y los riesgos que entraña el tratamiento para las personas interesadas.
- b) Se permite al contratista implementar medidas alternativas adecuadas en virtud del progreso tecnológico. En este sentido, el nivel de seguridad no podrá ser inferior al de las medidas establecidas en el apéndice III. Los cambios significativos deberán ser documentados.
- c) El contratista solo concederá a los miembros de su personal acceso a los datos personales tratados en la medida en que sea estrictamente necesario para la ejecución, la gestión y el seguimiento del contrato. El contratista garantizará que las personas autorizadas para tratar los datos personales recibidos se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria.

6.5 Datos sensibles

Si el tratamiento afecta a datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física, o datos relativos a condenas e infracciones penales (en lo sucesivo, “datos sensibles”), el contratista aplicará medidas adecuadas y específicas que se adapten a la naturaleza

específica de los datos y a los riesgos que entrañan. Entre estas medidas, pueden incluirse, por ejemplo, limitar el personal con acceso a los datos personales, o garantizar la capacidad, confidencialidad, integridad, disponibilidad y resiliencia de los sistemas y servicios.

6.6 Documentación y cumplimiento de las cláusulas

- a) El contratista resolverá con presteza y de forma adecuada las consultas del comitente relacionadas con el tratamiento con arreglo al presente pliego de cláusulas.
- b) El contratista pondrá a disposición del comitente, a petición de este, la información que el comitente necesite para llevar íntegramente el registro de las actividades de tratamiento en el sentido del artículo 30, apartado 1, del Reglamento (UE) 2016/679.
- c) El contratista informará inmediatamente al comitente sobre cualquier control o medida llevados a cabo por las autoridades de control, o en caso de que, en el marco de su competencia, una autoridad de control realice consultas, investigaciones o cualquier otro tipo de averiguaciones relativas al contratista.
- d) El contratista pondrá a disposición del comitente toda la información necesaria para demostrar el cumplimiento de las obligaciones contempladas en el presente pliego de cláusulas y que deriven directamente del Reglamento (UE) 2016/679. A instancia del comitente, el contratista permitirá y contribuirá a la realización de auditorías de las actividades de tratamiento cubiertas por el presente pliego de cláusulas, a intervalos razonables o si existen indicios de incumplimiento. Al decidir si se realiza un examen o una auditoría, el comitente podrá tener en cuenta las certificaciones pertinentes que obren en poder del contratista.
- e) El comitente podrá optar por realizar la auditoría por sí mismo o autorizar a un auditor independiente. Las auditorías también podrán consistir en inspecciones de los locales o instalaciones físicas del contratista y, cuando proceda, realizarse con un preaviso razonable.
- f) Las partes pondrán a disposición de la autoridad de control competente, a instancia de esta, la información a que se refiere la presente cláusula y, en particular, los resultados de las auditorías.

Cláusula 7. Recurso a subcontratistas

- a) El contratista solo podrá subcontratar a un subcontratista (otros encargados del tratamiento) las operaciones de tratamiento que realice por cuenta del comitente en virtud del presente pliego de cláusulas con la autorización previa documentada específica del comitente. El contratista presentará la solicitud de autorización específica al menos 20 días naturales antes de la contratación prevista del subcontratista de que se trate, junto con la información necesaria para que el comitente pueda resolver la solicitud. La información comprenderá al menos el nombre completo del subcontratista, incluidos la dirección y el país, así como una descripción del tratamiento por parte del subcontratista (incluidos el objeto, la naturaleza y la duración). El comitente autoriza la contratación de los subcontratistas mencionados en el apéndice II. Las partes mantendrán actualizado dicho apéndice.
- b) De excluirse la posibilidad de contratar a subcontratistas (otros encargados del tratamiento), el comitente lo establecerá así en el apéndice II.

- c) Cuando el contratista contrate a un subcontratista para llevar a cabo actividades de tratamiento específicas (por cuenta del comitente), lo hará por medio de un contrato que imponga al subcontratista, en esencia, las mismas obligaciones en materia de protección de datos que las impuestas al contratista en virtud del presente pliego de cláusulas. El contratista se asegurará de que el subcontratista cumpla las obligaciones a las que esté sujeto en virtud del presente pliego de cláusulas y del Reglamento (UE) 2016/679.
- d) El contratista proporcionará al comitente, a instancia de este, una copia del contrato con el subcontratista y de cualquier modificación posterior del mismo. En la medida en que sea necesario para proteger secretos comerciales u otro tipo de información confidencial, como datos personales, el contratista podrá expurgar el texto del contrato antes de compartir la copia.
- e) El contratista seguirá siendo plenamente responsable ante el comitente del cumplimiento de las obligaciones que imponga al subcontratista su contrato con el contratista. El contratista notificará al comitente los incumplimientos por parte del subcontratista de las obligaciones que le atribuya dicho contrato. En tal caso, el contratista, a instancia del comitente, deberá extinguir total o parcialmente la contratación del subcontratista o rescindir la relación contractual con el subcontratista cuando y en la medida en que esto no resulte desproporcionado.
- f) No se considerarán prestaciones de subcontratistas en el sentido del presente pliego de cláusulas aquellos servicios proporcionados por terceros a los que el contratista recurra como servicios auxiliares para respaldar la ejecución del encargo, como, por ejemplo, los servicios de telecomunicaciones. Sin embargo, para garantizar la protección y la seguridad de los datos del comitente, el contratista está obligado a tomar las medidas de control y a formalizar los acuerdos contractuales adecuados y conformes con la ley, incluso en el caso de servicios auxiliares externalizados.
- g) El contratista pactará con el subcontratista una cláusula de tercero beneficiario en virtud de la cual, en caso de que el contratista desaparezca de facto, cese de existir jurídicamente o sea insolvente, el comitente tendrá derecho a rescindir el contrato del subcontratista y ordenar a este que suprima o devuelva los datos personales.

Cláusula 8. Transferencias internacionales

- a) La prestación del tratamiento de datos acordado contractualmente tiene lugar exclusivamente en un Estado miembro de la Unión Europea o en otro Estado parte en el Acuerdo sobre el Espacio Económico Europeo.
- b) Las transferencias de datos a un tercer país o a una organización internacional por parte del contratista solo podrán realizarse siguiendo instrucciones documentadas del comitente o en virtud de una exigencia expresa del Derecho de la Unión o del Estado miembro al que esté sujeto el contratista; se llevarán a cabo de conformidad con el capítulo V del Reglamento (UE) 2016/679.

- c) El comitente se aviene a que, cuando el contratista recurra a un subcontratista de conformidad con la cláusula 7 para llevar a cabo actividades de tratamiento específicas (por cuenta del comitente) y dichas actividades conlleven una transferencia de datos personales en el sentido del capítulo V del Reglamento (UE) 2016/679, el contratista y el subcontratista puedan garantizar el cumplimiento del capítulo V del Reglamento (UE) 2016/679 utilizando cláusulas contractuales tipo adoptadas por la Comisión, con arreglo al artículo 46, apartado 2, del Reglamento (UE) 2016/679, siempre que se cumplan las condiciones para la utilización de dichas cláusulas contractuales tipo.

Cláusula 9. Ayuda al comitente

- a) El contratista notificará con presteza al comitente las solicitudes que reciba de la persona interesada. No responderá a dicha solicitud por sí mismo, a menos que el comitente le haya autorizado a hacerlo.
- b) El contratista ayudará al comitente a cumplir sus obligaciones al responder a las solicitudes de ejercicio de derechos de las personas interesadas teniendo en cuenta la naturaleza del tratamiento. En el cumplimiento de las obligaciones que le atribuyen las letras a) y b), el contratista cumplirá las instrucciones del comitente.
- c) Además de la obligación del contratista de ayudar al comitente en virtud de la cláusula 9, letra b), el contratista también ayudará al comitente a garantizar el cumplimiento de las obligaciones siguientes teniendo en cuenta la naturaleza del tratamiento y la información de que disponga el contratista:
1. la obligación de realizar una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales (en lo sucesivo, “evaluación de impacto relativa a la protección de los datos”) cuando sea probable que un tipo de tratamiento suponga un alto riesgo para los derechos y libertades de las personas físicas;
 2. la obligación de consultar a la autoridad de control competente antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos muestre que el tratamiento entrañaría un alto riesgo si el comitente no toma medidas para mitigarlo;
 3. la obligación de garantizar que los datos personales sean exactos y estén actualizados, informando sin demora al comitente si el contratista descubre que los datos personales que está tratando son inexactos o han quedado obsoletos;
 4. las obligaciones contempladas en el artículo 32 del Reglamento (UE) 2016/679.
- d) Las partes establecerán en el apéndice III medidas técnicas y organizativas apropiadas que obliguen al contratista a ayudar al comitente a aplicar la presente cláusula, así como el objeto y el alcance de la ayuda requerida.

Cláusula 10. Notificación de violaciones de la seguridad de los datos personales

En caso de violación de la seguridad de los datos personales, el contratista colaborará con el comitente y le ayudará a cumplir las obligaciones que le atribuyen los artículos 33 y 34 del Reglamento (UE) 2016/679, teniendo en cuenta la naturaleza del tratamiento y la información de que disponga el contratista.

10.1 Violación de la seguridad de datos personales tratados por el responsable

En caso de violación de la seguridad de los datos personales en relación con los datos tratados por el comitente, el contratista ayudará al comitente en lo siguiente.

- a) Notificar la violación de la seguridad de los datos personales a la autoridad de control competente sin dilación indebida una vez el comitente tenga constancia de ella, si procede (a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas).
- b) Recabar la información siguiente, que, de conformidad con el artículo 33, apartado 3, del Reglamento (UE) 2016/679, deberá figurar en la notificación del comitente, que debe incluir como mínimo:
 - 1) la naturaleza de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de personas interesadas afectadas, y las categorías y el número aproximado de registros de datos personales afectados;
 - 2) las consecuencias probables de la violación de la seguridad de los datos personales;
 - 3) las medidas adoptadas o propuestas por el comitente para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Cuando y en la medida en que no se pueda proporcionar toda la información al mismo tiempo, en la notificación inicial se proporcionará la información de que se disponga en ese momento y, a medida que se vaya recabando, la información adicional se irá proporcionando sin dilación indebida.

- c) Cumplir, con arreglo al artículo 34 del Reglamento (UE) 2016/679, la obligación de comunicar sin dilación indebida a la persona interesada la violación de la seguridad de los datos personales cuando sea probable que la violación de la seguridad entrañe un alto riesgo para los derechos y libertades de las personas físicas.

10.2 Violación de la seguridad de datos personales tratados por el contratista

En caso de violación de la seguridad de datos personales tratados por el contratista, este lo notificará al comitente sin dilación indebida una vez que el contratista tenga constancia de ella. Dicha notificación deberá incluir como mínimo:

- a) una descripción de la naturaleza de la violación de la seguridad (inclusive, cuando sea posible, las categorías y el número aproximado de personas interesadas y de registros de datos afectados);

- b) los datos de un punto de contacto en el que pueda obtenerse más información sobre la violación de la seguridad de los datos personales;
- c) sus consecuencias probables y las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad, incluyendo las medidas adoptadas para mitigar los posibles efectos negativos.

Cuando y en la medida en que no se pueda proporcionar toda la información al mismo tiempo, en la notificación inicial se proporcionará la información de que se disponga en ese momento y, a medida que se vaya recabando, la información adicional se irá proporcionando sin dilación indebida.

Las partes establecerán en el apéndice III los demás elementos que deberá aportar el contratista cuando ayude al comitente a cumplir las obligaciones que le atribuyen los artículos 33 y 34 del Reglamento (UE) 2016/679.

Cláusula 11. Incumplimiento de las cláusulas y resolución del contrato

- a) Sin perjuicio de lo dispuesto en el Reglamento (UE) 2016/679, en caso de que el contratista incumpla las obligaciones que le atribuye el presente pliego de cláusulas, el comitente podrá ordenar al contratista que suspenda el tratamiento de datos personales hasta que este vuelva a dar cumplimiento al presente pliego de cláusulas o finalice el contrato. El contratista informará con presteza al comitente en caso de que no pueda dar cumplimiento al presente pliego de cláusulas por cualquier motivo.
- b) El comitente estará facultado para resolver el contrato en lo que se refiera al tratamiento de datos personales en virtud del presente pliego de cláusulas cuando:
 - 1) el tratamiento de datos personales por parte del contratista haya sido suspendido por el comitente con arreglo a la letra a) y no se vuelva a dar cumplimiento al presente pliego de cláusulas en un plazo razonable y, en cualquier caso, en un plazo de un mes a contar desde la suspensión;
 - 2) el contratista incumpla de manera sustancial o persistente el presente pliego de cláusulas o las obligaciones que le atribuye el Reglamento (UE) 2016/679;
 - 3) el contratista incumpla una resolución vinculante de un órgano jurisdiccional competente o de la autoridad de control competente en relación con las obligaciones que les atribuye el presente pliego de cláusulas o el Reglamento (UE) 2016/679;

De conformidad con el apartado 5.3.2 de las Condiciones Contractuales Generales (CCG), si el comitente resolviera el contrato por alguno de los motivos anteriormente mencionados, la resolución será imputable al contratista.

- c) El contratista estará facultado para resolver el contrato en lo que se refiera al tratamiento de datos personales en virtud del presente pliego de cláusulas cuando, tras haber informado al comitente de que sus instrucciones infringen los requisitos jurídicos exigidos por la cláusula 6.1, letra b), el comitente insista en que se sigan dichas instrucciones.
- d) Tras la resolución del contrato, el contratista devolverá al comitente todos los datos personales tratados por cuenta del comitente y suprimirá las copias existentes, a menos que el Derecho de la Unión o de los Estados miembros exija el almacenamiento de los

datos personales. Hasta que se destruyan o devuelvan los datos, el contratista seguirá garantizando el cumplimiento con el presente pliego de cláusulas.

- e) Los soportes de datos y registros de datos cedidos seguirán siendo propiedad del comitente.

Apéndice I. Descripción del tratamiento

La siguiente selección ha sido realizada por el comitente. Si en el marco del procedimiento de adjudicación o de la ejecución de la orden el contratista detectase lagunas, errores o ambigüedades, deberá comunicárselo al comitente.

Naturaleza, finalidad y duración del tratamiento

- ☒ El objeto y la duración del tratamiento de datos subcontratado, así como el alcance y la naturaleza del tratamiento de los datos personales se rigen por los términos de referencia, así como por la oferta presentada por el contratista.
- ☐ Descripción más detallada del alcance, la naturaleza y la finalidad del tratamiento:

Categorías de personas interesadas cuyos datos personales se tratan

- ☐ Colaboradores y colaboradoras del comitente, incluidos los candidatos y candidatas a puestos de trabajo
- ☐ Suscriptores y suscriptoras, por ejemplo, de revistas y boletines de noticias
- ☒ Participantes externos y externas en eventos
- ☐ Participantes en encuestas
- ☐ Visitantes de locales del comitente
- ☐ Visitantes de sitios web
- ☐ Proveedores de bienes / de servicios
- ☒ Personas de contacto de instituciones contraparte
- ☒ Representantes de entidades públicas y representantes gubernamentales
- ☐ Estudiantes / becarios y becarias
- ☐ Otras categorías:

Categorías de datos personales tratados

- ☒ Datos personales básicos (nombre, fecha de nacimiento)
- ☐ Datos de dirección postal
- ☒ Datos de contacto y comunicación (p. ej., teléfono, dirección de correo electrónico, etc.)
- ☐ Datos relativos a la cualificación (p. ej., trayectorias profesionales, currículos, cualificaciones, etc.)
- ☐ Datos relativos al empleo (datos salariales, datos bancarios, régimen fiscal, etc.)
- ☐ Datos de facturación y pago
- ☐ Datos de usuario / usuaria (datos de navegación, direcciones IP, *cookies*, nombres de usuario / usuaria, etc.)
- ☒ Datos de imagen y de audio
- ☐ Datos de viaje y de localización
- ☐ Categorías especiales de datos personales de conformidad con el artículo 9 del Reglamento (UE) 2016/679 (p. ej., datos relativos a la salud, datos biométricos, datos que revelen el origen étnico, las convicciones religiosas, políticas o filosóficas o datos sobre la vida sexual o la orientación sexual de una persona física)
- ☐ Otras categorías:

Apéndice II. Lista de subcontratistas

- ☒ El contratista solo podrá subcontratar a un subcontratista las operaciones de tratamiento que realice por cuenta del comitente en virtud del presente pliego de cláusulas.

El comitente autoriza la contratación de los siguientes subcontratistas:

Nombre	Dirección, incluido el país	Descripción del tratamiento (incluido el objeto, la naturaleza y la duración)	En el caso de transferencia de datos a un tercer país o a una organización internacional, ¿cómo se garantiza el cumplimiento del capítulo V del Reglamento (UE) 2016/679?

Apéndice III. Medidas técnicas y organizativas, en especial medidas técnicas y organizativas para garantizar la seguridad de los datos

Descripción de las medidas de seguridad técnicas y organizativas aplicadas por el contratista (inclusive las certificaciones pertinentes) para garantizar un nivel adecuado de seguridad, teniendo en cuenta la naturaleza, el alcance, el contexto y la finalidad del tratamiento, así como los riesgos para los derechos y libertades de las personas físicas.

Para la exposición, puede utilizarse la siguiente lista de verificación, que incluye un gran número de posibles medidas técnicas y organizativas. La lista de verificación no es exhaustiva y deberá completarse por parte del contratista en cada caso individual siempre que sea necesario. Para garantizar una descripción precisa, deberán añadirse las correspondientes notas aclaratorias.

Como alternativa, la exposición y descripción de las medidas técnicas y organizativas adoptadas por el contratista también puede efectuarse en un documento separado.

1. Medidas de seudonimización y cifrado de los datos personales

- ☐ Seudonimización de los datos personales que dejen de ser necesarios de forma visible
- ☐ Directriz sobre seudonimización
- ☐ Cifrado de soportes de datos
- ☐ Seudonimización de datos en sistemas de prueba
- ☐ Cifrado de sitios web (SSL)
- ☐ Cifrado de bases de datos
- ☐ Cifrado de correo electrónico (TLS 1.2 o 1.3)
- ☐ Cifrado de contraseñas y claves
- ☐ Cifrado de dispositivos móviles
- ☐ 

Nota aclaratoria: 

2. Medidas para garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento

- ☐ Acuerdos de confidencialidad con los colaboradores y colaboradoras
- ☐ Obligación en materia de protección de datos de los colaboradores y colaboradoras
- ☐ Acuerdo de no divulgación con terceros
- ☐ Sistemas de almacenamiento externo / servidores de respaldo
- ☐ Contratos de soporte con terceros
- ☐ Acuerdos de externalización de la gestión de datos
- ☐ Uso de proveedores certificados de servicios en la nube
- ☐ Cortafuegos
- ☐ Programa antivirus
- ☐ Aseguramiento de datos periódico
- ☐ Sistemas redundantes
- ☐ Vigilancia de sistemas y servicios
- ☐ Sistemas de almacenamiento con RAID

- ☐ Sistemas de almacenamiento conectado en red (NAS)
- ☐ Contratos de mantenimiento
- ☐ Test periódicos de averías informáticas
- ☐ Almacenamiento interno de copias / copias de seguridad
- ☐ Sistemas de alimentación ininterrumpida (SAI)
- ☐ Sistemas de detección de incendios y de humo
- ☐ Equipos para el control de temperaturas
- ☐ Equipamiento para la extinción de incendios
- ☐ Sistema de alarma contra el acceso no autorizado
- ☐ Tecnología de equilibrio de carga
- ☐ [REDACTED]

Nota aclaratoria: [REDACTED]

3. Medidas para restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico

- ☐ Realización periódica de copias de seguridad de todo el sistema
- ☐ Almacenamiento en varios sistemas
- ☐ Estrategia de aseguramiento de datos
- ☐ Test periódico de copia de seguridad / recuperación
- ☐ Contratos de soporte y asistencia de *hardware*
- ☐ Estrategia de gestión de emergencias
- ☐ Aseguramiento de datos externalizado
- ☐ Capacitación regular del personal de TI
- ☐ [REDACTED]

Nota aclaratoria: [REDACTED]

4. Procesos de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento

- ☐ Controles internos
- ☐ Control de contratos (selección meticulosa de los contratistas, formulación clara del contrato, etc.)
- ☐ Verificación periódica de los procesos informáticos
- ☐ Auditorías periódicas (p. ej., por parte del delegado o la delegada para la protección de datos)
- ☐ Verificación periódica de los procedimientos
- ☐ Auditoría de las medidas técnicas y organizativas por parte del delegado o la delegada para la protección de datos
- ☐ Chequeos regulares de los colaboradores y colaboradoras
- ☐ Realización de evaluaciones de impacto relativas a la protección de datos
- ☐ Chequeo del diseño técnico / las configuraciones por defecto
- ☐ Sistema de gestión de protección de datos / manual de protección de datos
- ☐ 

Nota aclaratoria: 

5. Medidas para la identificación y autorización de los usuarios y usuarias

- ☐ Autenticación de dos factores
- ☐ Autenticación con nombre de usuario o usuaria y contraseña
- ☐ Separación de roles de los sistemas de prueba y productivo
- ☐ Verificación periódica de las autorizaciones
- ☐ Contraseñas para el BIOS
- ☐ Estrategia de autorizaciones
- ☐ Directriz sobre la administración de dispositivos móviles
- ☐ Perfiles de usuario o usuaria
- ☐ Directriz sobre contraseñas
- ☐ Limitación del número de administradores y administradoras
- ☐ Identificación de nuevos colaboradores y colaboradoras
- ☐ Separación de los roles de usuario o usuaria
- ☐ Mecanismos automáticos de bloqueo
- ☐ Identificación de personas externas mediante tarjetas identificativas
- ☐ Administración de los derechos por parte de un administrador o una administradora
- ☐ Diferenciación entre autorizaciones
- ☐ 

Nota aclaratoria: 

6. Medidas para la protección de los datos durante la transmisión

- ☐ Uso de tecnologías de cifrado
- ☐ Redes privadas virtuales (VPN)
- ☐ Sistema de registro de actividades e incidentes
- ☐ Transmisión mediante una nube privada
- ☐ Documentación de los receptores y receptoras de datos
- ☐ Cifrado de correo electrónico (TLS 1.2 o 1.3)
- ☐ Verificación de la identidad de los receptores y receptoras de datos
- ☐ Uso de unidades de disco no públicas
- ☐ Transporte físico: contenedores seguros para el transporte
- ☐ Selección meticulosa del personal de transporte
- ☐ 

Nota aclaratoria: 

7. Medidas para la protección de los datos durante el almacenamiento

- ☐ Cifrado de soportes de datos
- ☐ Clasificación de los datos
- ☐ Estrategia de autorizaciones
- ☐ Restricciones de acceso
- ☐ Sistema de registro de acciones e incidentes
- ☐ Puertas de seguridad
- ☐ Limitación del número de administradores y administradoras
- ☐ Acceso mediante tarjeta llave / acceso RFID
- ☐ Anonimización de datos
- ☐ Seudonimización de datos
- ☐ Conservación segura de los soportes de datos
- ☐ Cortafuegos
- ☐ 

Nota aclaratoria: 

8. Medidas para garantizar la seguridad física de los lugares en los que se tratan los datos personales

- ☐ Sistema de alarma
- ☐ Control de personas / conserje
- ☐ Protección de los huecos de edificio
- ☐ Sistema de registro de los y las visitantes
- ☐ Control automatizado del acceso
- ☐ Selección meticulosa del personal de limpieza
- ☐ Selección meticulosa del personal de seguridad
- ☐ Tarjetas inteligentes, transpondedores

- ☐ Sistema de cierre con cerradura de código
- ☐ Obligación de llevar tarjetas identificativas de autorización
- ☐ Sistema de cierre manual
- ☐ Estrategia de acceso
- ☐ Bloqueo biométrico
- ☐ Armarios de servidores con llave
- ☐ Videovigilancia de las entradas
- ☐ Puertas con un pomo en el lado exterior
- ☐ Sensores fotoeléctricos / detectores de movimiento
- ☐ Visitantes: siempre en compañía de colaboradores o colaboradoras
- ☐ Cerraduras de seguridad
- ☐ Portero automático con cámara
- ☐ Procedimiento de entrega de llaves
- ☐ 

Nota aclaratoria: 

9. Medidas para garantizar el registro de incidentes

- ☐ Uso de un sistema de registro automatizado
- ☐ Elaboración de informes de incidentes
- ☐ Notificación con alarma en tiempo real
- ☐ Sistema de registro a nivel de la aplicación
- ☐ Verificación automatizada de los protocolos
- ☐ Sincronización de los relojes del sistema
- ☐ Verificación manual periódica de los protocolos
- ☐ Consolidación automatizada de los incidentes
- ☐ Los protocolos se guardan en la aplicación y se envían automáticamente a otro lugar
- ☐ 

Nota aclaratoria: 

10. Medidas para garantizar la configuración del sistema, en especial la configuración por defecto

- ☐ Se cuenta con una directriz de gestión de la configuración
- ☐ Proceso para las modificaciones de la configuración
- ☐ Ajustes predeterminados conformes a la legislación sobre protección de datos
- ☐ Chequeo de las configuraciones por defecto
- ☐ Definición de las configuraciones por defecto
- ☐ Configuración por parte del administrador o de la administradora del sistema
- ☐ Sistema de registro de las modificaciones de la configuración
- ☐ Capacitación regular del personal de TI
- ☐ [REDACTED]

Nota aclaratoria: [REDACTED]

11. Medidas de gobernanza y gestión de la informática y la seguridad informática internas

- ☐ Directriz de seguridad informática
- ☐ Directriz de administración informática
- ☐ Auditorías / verificaciones periódicas en relación con el cumplimiento
- ☐ Inventario de equipos informáticos
- ☐ Capacitación del personal en materia de seguridad de los datos
- ☐ Verificación / evaluación periódica de sistemas
- ☐ Equipo de TI con asignación de roles / responsabilidades
- ☐ Directrices para la gestión de incidentes
- ☐ Evaluación del riesgo y medidas de gestión del riesgo en todos los niveles y fases ☐

Nota aclaratoria: [REDACTED]

12. Medidas para la certificación / garantía de procesos y productos

- ☐ Implantación de la norma ISO 9001 (gestión de la calidad)
- ☐ Implantación de la norma ISO 27001 (gestión de seguridad de la información)
- ☐ Implementación de la norma ISO 27701 (gestión de la privacidad de la información)
- ☐ Certificación relativa al RGPD (gestión de protección de datos)
- ☐ Visión de conjunto de las disposiciones vigentes para productos / servicios / procesos
- ☐ Identificación de estándares específicos del sector
- ☐ Auditorías internas y/o externas periódicas
- ☐ Asignación de responsabilidades de auditoría a expertos y expertas certificados
- ☐ Verificación periódica de nuevas condiciones y de la renovación de certificados
- ☐ [REDACTED]

Nota aclaratoria: [REDACTED]

13. Medidas para garantizar la minimización de datos

- ☐ Identificación de la finalidad del tratamiento
- ☐ Valoración de la relación entre el tratamiento y la finalidad
- ☐ Evaluación del alcance y de la calidad de los datos tratados en relación con la finalidad
- ☐ Identificación de los plazos de conservación aplicables
- ☐ Supresión segura de los datos una vez vencido el plazo de conservación
- ☐ 

Nota aclaratoria: 

14. Medidas para garantizar la calidad de los datos

- ☐ Creación de perfiles y clasificación de datos
- ☐ Controles para los datos entrantes o nuevos
- ☐ Sistema de registro de la introducción / modificación de datos
- ☐ Asignación de derechos para la introducción de datos
- ☐ Conservación de protocolos
- ☐ Trazabilidad de los usuarios y usuarias que introducen y modifican datos (sin grupos de usuarios y usuarias)
- ☐ Prevención de datos duplicados
- ☐ Identificación de requisitos para los datos
- ☐ Aplicación de medidas para garantizar la calidad de los datos
- ☐ 

Nota aclaratoria: 

15. Medidas para garantizar una retención limitada de los datos

- ☐ Directriz sobre conservación con inclusión de roles
- ☐ Separación de los datos en función de los plazos de conservación
- ☐ Capacitaciones regulares
- ☐ Verificación y evaluación periódica de los datos almacenados
- ☐ 

Nota aclaratoria: 

16. Medidas para garantizar la responsabilidad proactiva

- ☐ Capacitaciones / sensibilización
- ☐ Controles y exámenes periódicos
- ☐ Existencia de un equipo de protección de datos
- ☐ Orientación y apoyo a los colaboradores y colaboradoras
- ☐ Directrices sobre protección de datos adecuadas
- ☐ Celebración de cláusulas contractuales tipo
- ☐ Acuerdos sobre responsabilidad compartida
- ☐ Respuesta a las consultas de las personas interesadas
- ☐ Documento de transparencia (artículos 13 y 14 del RGPD)
- ☐ Supresión segura de los datos
- ☐ Declaración de protección de datos documentada
- ☐ Los informes de las auditorías y las medidas están documentados
- ☐ Se involucra debidamente al delegado o a la delegada para la protección de datos
- ☐ Procedimiento de consentimiento específico / conservación de las actas de consentimiento
- ☐ [Redacted]

Nota aclaratoria: [Redacted]

17. Medidas para permitir la portabilidad de los datos y garantizar la supresión

- ☐ Almacenamiento en un formato estructurado
- ☐ Vigilancia de los plazos legales
- ☐ Transferencia mediante cifrado de extremo a extremo
- ☐ Cumplimiento de plazos de conservación
- ☐ Se posibilita la portabilidad de los datos
- ☐ Los derechos de las personas interesadas se tratan de conformidad con el capítulo 3 del Reglamento (UE) 2016/679
- ☐ Se garantiza una supresión segura de los datos
- ☐ Se garantiza una destrucción segura de los soportes de datos
- ☐ [Redacted]

Nota aclaratoria: [Redacted]