ANEXO II: CONTRATACIÓN, POR LA CONSELLERÍA DE SANIDADE, DE LOS SERVICIOS DE SOPORTE, MANTENIMIENTO Y EVOLUCIÓN DE LAS APLICACIONES DE SALUD PÚBLICA Y PLANIFICACIÓN SANITARIA

Índice

1 INTRODUCCIÓN.

2 PROTECCIÓN DE DATOS

2.1 NORMATIVA

De conformidad con la Disposición adicional 25ª de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014, los contratos que impliquen el tratamiento de datos de carácter personal deberán respetar en su integridad el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales (RGPD), y la normativa complementaria.

Para el caso de que la contratación implique el acceso del contratista a datos de carácter personal de cuyo tratamiento sea responsable la entidad contratante, aquél tendrá la consideración de encargado del tratamiento. En este supuesto, el acceso a esos datos no se considerará comunicación de datos, cuando se cumpla lo previsto en el artículo 28 del RGPD. En todo caso, las previsiones de este deberán de constar por escrito.

2.2 TRATAMIENTO DE DATOS PERSONALES

Para el cumplimiento del objeto de esta licitación, el adjudicatario deberá tratar los datos personales de los cuales la Consellería de Sanidad es Responsable del Tratamiento.

Ello conlleva que el adjudicatario actúe en calidad de Encargado del Tratamiento y, por tanto, tiene el deber de cumplir con la normativa vigente en cada momento, tratando y protegiendo debidamente los Datos Personales.

Por tanto, sobre la la Consejería de Sanidad recaen las responsabilidades del Responsable del Tratamiento y sobre el adjudicatario las de Encargado de Tratamiento. Si el adjudicatario destinase los datos a otra finalidad, los comunicara o los utilizara incumpliendo las estipulaciones del contrato y/o la normativa vigente, será considerado también como Responsable del Tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

En caso de que como consecuencia de la ejecución del contrato resultara necesario en algún momento la modificación del contrato, el adjudicatario lo requerirá razonadamente y señalará los cambios que solicita. En caso de que la la Consejería de Sanidad estuviese de acuerdo con lo solicitado se generaría un contrato actualizado, de modo que el mismo siempre recoja fielmente el detalle del tratamiento.

2.3 IDENTIFICACIÓN DE LA INFORMACIÓN AFECTADA.

Para la ejecución de las prestaciones derivadas de la presente licitación, la Consellería de Sanidade, responsable del tratamiento, pondrá a disposición del adjudicatario -encargado de tratamiento-, la información descrita en el documento de registro de actividades de tratamiento publicado en la URL: http://www.sergas.gal/protecciondatos, siendo susceptible de tratamiento cualquiera de las actividades en él recogidas, ya que todas implican uso de sistemas de información y todas ellas dentro del alcance del sistema de gestión de calidad implantado.

Se realizará recogida, registro, conservación, consulta, supresión y destrucción de la información.

3 OBLIGACIONES DEL ENCARGADO DEL TRATAMIENTO (ESTIPULACIONES COMO ENCARGADO DE TRATAMIENTO)

De conformidad con lo previsto en el artículo 28 del RGPD, el adjudicatario y todo su personal se obliga a y garantiza el cumplimiento de las siguientes

3.1.1 Tratar los Datos Personales conforme a las instrucciones documentadas en el presente contrato o demás documentos contractuales aplicables a la ejecución del contrato y aquellas que, en su caso, reciba de AEPD por escrito en cada momento.

El adjudicatario informará inmediatamente a la Consejería de Sanidad cuando, en su opinión, una instrucción sea contraria a la normativa de protección de Datos Persona-les aplicable en cada momento.

3.1.2 Utilizar los datos personales objeto de tratamiento, o los que recoja para su inclusión, sólo para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para fines propios.

3.1.3 Tratar los Datos Personales de conformidad con los criterios de seguridad y el contenido previsto en el artículo 32 del RGPD, así como observar y adoptar las medidas técnicas y organizativas de seguridad necesarias o convenientes para asegurar la confidencialidad, secreto e integridad de los Datos Personales a los que tenga acceso.

Si el encargado del tratamiento considera que alguna de las instrucciones infringe el RGPD o cualquier otra disposición en materia de protección de datos de la Unión o de los Estados miembros, el encargado informará inmediatamente al responsable.

3.1.4 Llevar, por escrito, un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable, que contenga:

- El nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado y, en su caso, del representante

del responsable o del encargado y del delegado de protección de datos.

- Las categorías de tratamientos efectuados por cuenta de cada responsable.
- En su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49 apartado 1, párrafo segundo del RGPD, la documentación de garantías adecuadas.
- Una descripción general de las medidas técnicas y organizativas de seguridad relativas a:
  - La seudoanimización y el cifrado de datos personales.
  - La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento
  - La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
  - El proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

3.1.5 El adjudicatario y todo su personal se obliga mantener la más absoluta confidencialidad sobre los Datos Personales a los que tenga acceso para la ejecución del contrato así como sobre los que resulten de su tratamiento, cualquiera que sea el soporte en el que se hubieren obtenido. Esta obligación se extiende a toda persona que pudiera intervenir en cualquier fase del tratamiento por cuenta del adjudicatario, siendo deber del adjudicatario instruir a las personas que de él dependan, de este deber de secreto, y del mantenimiento de dicho deber aún después de la terminación de la prestación del Servicio o de su desvinculación.

Llevar un listado de personas autorizadas para tratar los Datos Personales objeto de este contrato y garantizar que las mismas se comprometen, de forma expresa y por escrito, a respetar la confidencialidad, y a cumplir con las medidas de seguridad correspondientes, de las que les debe informar convenientemente. Y mantener a disposición de la Consejería de Sanidad dicha documentación acreditativa.

3.1.6 Salvo que cuente en cada caso con la autorización expresa del Responsable del Tratamiento dentro de los supuestos legalmente admisibles, no comunicar (ceder) ni difundir los Datos Personales a terceros, ni siquiera para su conservación.

El encargado puede comunicar los datos a otros encargados del tratamiento del mismo responsable, de acuerdo con las instrucciones del responsable. En este caso, el responsable identificará, de forma previa y por escrito, la entidad a la que se deben

comunicar los datos, los datos a comunicar y las medidas de seguridad a aplicar para proceder a la comunicación.

Si el encargado debe transferir datos personales a un tercer país o a una organización internacional, en virtud del Derecho de la Unión o de los Estados miembros que le sea aplicable, informará al responsable de esa exigencia legal de manera previa, salvo que tal Derecho lo prohíba por razones importantes de interés público.

3.1.7 No se permite subcontratar ninguna de las prestaciones que formen parte del objeto de este contrato que comporten el tratamiento de datos personales, salvo los servicios auxiliares necesarios para el normal funcionamiento de los servicios del encargado.

Si fuera necesario subcontratar algún tratamiento, este hecho se deberá comunicar previamente y por escrito al responsable, indicando los tratamientos que se pretende subcontratar e identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto. La subcontratación podrá llevarse a cabo si el responsable lo autoriza. La no respuesta del responsable de tratamiento a dicha solicitud por el contratista equivale a oponerse a dichos cambios.

El subcontratista, que también tendrá la condición de encargado del tratamiento, está obligado igualmente a cumplir las obligaciones establecidas en este documento para el encargado del tratamiento y las instrucciones que dicte el responsable. Corresponde al encargado inicial regular la nueva relación de forma que el nuevo encargado quede sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad...) y con los mismos requisitos formales que él, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas. En el caso de incumplimiento por parte del subencargado, el encargado inicial seguirá siendo plenamente responsable ante el responsable en lo referente al cumplimiento de las obligaciones.

En todo caso, para autorizar la contratación, es requisito imprescindible que se cumplan las siguientes condiciones (si bien, aun cumpliéndose las mismas, corresponde al responsable de tratamiento la decisión de si otorgar, o no, dicho consentimiento):

- Que el tratamiento de datos personales por parte del subcontratista se ajuste a la legalidad vigente, lo contemplado en este pliego y a las instrucciones del responsable de tratamiento.
- Que el adjudicatario y la empresa subcontratista formalicen un contrato de encargo de tratamiento de datos en términos no menos restrictivos a los previstos en el presente contrato, el cual será puesto a disposición del responsable de tratamiento a su mera solicitud para verificar su existencia y contenido.

El adjudicatario informará al responsable de tratamiento. de cualquier cambio previsto en la incorporación o sustitución de otros subcontratistas, dando así al responsable de tratamiento. la oportunidad de otorgar el consentimiento previsto en esta cláusula. La no respuesta del responsable de tratamiento. a dicha solicitud por el contratista equivale a oponerse a dichos cambios

3.1.8 Mantener a disposición del responsable la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.

3.1.9 Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.

3.1.10 Designar un delegado de protección de datos y comunicar su identidad y datos de contacto al responsable.

3.1.11 Cuando una persona ejerza un derecho (de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones individualizadas automatizadas, u otros reconocidos por la normativa aplicable (conjuntamente, los "Derechos"), ante el Encargado del Tratamiento, éste debe comunicarlo al responsable de tratamiento por correo electrónico a la dirección delegado.proteccion.datos@sergas.es con la mayor prontitud. La comunicación debe hacerse de forma inmediata y en ningún caso más allá del día laborable siguiente al de la recepción del ejercicio de derecho, juntamente, en su caso, con la documentación y otras informaciones que puedan ser relevantes para resolver la solicitud que obre en su poder.

Asistirá al responsable de tratamiento, siempre que sea posible, para que ésta pueda cumplir y dar respuesta a los ejercicios de Derechos.

3.1.12 Una vez finalizada la prestación contractual objeto del presente contrato, se compromete, según corresponda, a devolver o destruir: (i) los Datos Personales a los que haya tenido acceso; (ii) los Datos Personales generados por el adjudicatario por causa del tratamiento; y (iii) los soportes y documentos en que cualquiera de estos datos consten, sin conservar copia alguna; salvo que se permita o requiera por ley o por norma de derecho comunitario su conservación, en cuyo caso no procederá la destrucción.

El Encargado del Tratamiento podrá, no obstante, conservar los datos durante el tiempo que puedan derivarse responsabilidades de su relación con el Responsable del Tratamiento. En este último caso, los Datos Personales se conservarán bloqueados y por el tiempo mínimo, destruyéndose de forma segura y definitiva al final de dicho plazo.

La devolución se realizará al finalizar el contrato o si lo requiere previamente el responsable de tratamiento o en quien delegue.

3.1.13 Corresponde al responsable facilitar el derecho de información en el momento de la recogida de los datos. En el caso de que la recogida de los datos la realice de forma directa el encargado del tratamiento, en el momento de la recogida de los datos, debiendo facilitar la información relativa a los tratamientos de datos que se van a realizar. La redacción y el formato en que se facilitará la información se debe consensuar con el responsable antes del inicio de la recogida de los datos.

3.1.14 De conformidad con el artículo 33 RGPD, comunicar al responsable de tratamiento, de forma inmediata y a más tardar en el plazo de **18 horas**, cualquier violación de la seguridad de los datos personales a su cargo de la que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia o cualquier fallo en su sistema de tratamiento y gestión de la información que haya tenido o pueda tener que ponga en peligro la seguridad de los Datos Personales, su integridad o su disponibilidad, así como cualquier posible vulneración de la confidencialidad como consecuencia de la puesta en conocimiento de terceros de los datos e informaciones obtenidos durante la ejecución del contrato. Comunicará con diligencia información detallada al respecto, incluso concretando qué interesados sufrieron una pérdida de confidencialidad.

Si se dispone de ella se facilitará, como mínimo, la información siguiente:

- Descripción de la naturaleza de la violación de la seguridad de los datos personales,inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.
- El nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.
- Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.
- Descripción de las medidas adoptadas o propuestas 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.
- Si no es posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

3.1.15 Poner disposición del responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen el responsable u otro auditor autorizado por él.

Disponer de evidencias que demuestren su cumplimiento de la normativa de protección de Datos Personales y del deber de responsabilidad activa, como, a título de ejemplo, certificados previos sobre el grado de cumplimiento o resultados de auditorías, que habrá

de poner a disposición del responsable de tratamiento a requerimiento de esta. Asimismo, durante la vigencia del contrato, pondrá a disposición del responsable de tratamiento toda información, certificaciones y auditorías realizadas en cada momento.

3.1.16 Las medidas de seguridad (en el Marco organizativo,Marco operacional y medidas de protección) están establecidas en el anexo II del Esquema Nacional de Seguridad que, aprobado mediante Real Decreto 3/2010, de 8 de enero y modificado a través del Real Decreto 951/2015, de 23 de octubre.

Antes de iniciar el tratamiento de datos se debe contactar con la Subdirección xeral de sistemas e tecnoloxías da información de cara a que esta pueda valorar el mismo.

En todo caso, deberán implantar mecanismos entre otros para:

- Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
- Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
- Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.
- Seudonimizar y cifrar los datos personales, en su caso.
- Designar un delegado de protección de datos12 y comunicar su identidad y datos de contacto al responsable.

3.1.17 Dar apoyo al responsable del tratamiento en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando proceda.

3.1.18 Dar apoyo al responsable del tratamiento en la realización de las consultas previas a la autoridad de control, cuando proceda.

3.1.19 Colaborar con el responsable de tratamiento en el cumplimiento de sus obligaciones en materia de (i) medidas de seguridad, (ii) comunicación y/o notificación de brechas (logradas e intentadas) de medidas de seguridad a las autoridades competentes o los interesados, y (iii) colaborar en la realización de evaluaciones de impacto relativas a la protección de datos personales y consultas previas al respecto a las autoridades competentes; teniendo en cuenta la naturaleza del tratamiento y la información de la que disponga.

El cumplimiento de esta obligación queda supeditado a la naturaleza del tratamiento realizado y a la información que esté a disposición del encargado.

Asimismo, pondrá a disposición del responsable, a requerimiento de éste, toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas y

colaborará en la realización de auditoras e inspecciones llevadas a cabo por el responsable o por otro auditor autorizado por el responsable.

3.1.20 Salvo que se indique otra cosa por parte del responsable de tratamiento se debe llevar a cabo el tratamiento de los Datos Personales en los sistemas/dispositivos de tratamiento, manuales y automatizados, y en las ubicaciones que en el responsable de tratamiento especifique, equipamiento que podrá estar bajo el control del responsable de tratamiento o bajo el control directo o indirecto del adjudicatario, u otros que hayan sido expresamente autorizados por escrito por el responsable, según se establezcan en su caso, y únicamente por los usuarios o perfiles de usuarios asignados a la ejecución del objeto de este contrato.

3.1.21 Salvo que se indique otra cosa por parte del responsable de tratamiento se deben tratar los Datos Personales dentro del Espacio Económico Europeo u otro espacio considerado por la normativa aplicable como de seguridad equivalente, no tratándolos fuera de este espacio ni directamente ni a través de cualesquiera subcontratistas autorizados conforme a lo establecido en este contrato o demás documentos contractuales, salvo que esté obligado a ello en virtud del Derecho de la Unión o del Estado miembro que le resulte de aplicación.

En el caso de que por causa de Derecho nacional o de la Unión Europea el adjudicatario se vea obligado a llevar a cabo alguna transferencia internacional de datos, el adjudicatario informará por escrito al responsable de tratamiento de esa exigencia legal, con antelación suficiente a efectuar el tratamiento, y garantizará el cumplimiento de cualesquiera requisitos legales que sean aplicables a la AEPD, salvo que el Derecho aplicable lo prohíba por razones importantes de interés público.

Las presentes cláusulas y las obligaciones en ella establecidas, constituyen el contrato de encargo de tratamiento entre el Responsable de tratamiento y el adjudicatario a que hace referencia el artículo 28.3 RGPD. Las obligaciones y prestaciones que aquí se contienen no son retribuibles de forma distinta de lo previsto en los documentos contractuales y tendrán la misma duración que la prestación de Servicio objeto del contrato, prorrogándose en su caso por períodos iguales a éste. No obstante, a la finalización del contrato, el deber de secreto continuará vigente, sin límite de tiempo, para todas las personas involucradas en la ejecución del contrato.

Para el cumplimiento del objeto de este contrato no se requiere que el adjudicatario acceda a ningún otro Dato Personal responsabilidad de el encargado de tratamiento, y por tanto no está autorizado en caso alguno al acceso o tratamiento de otro dato, que no sean los especificados en el contrato. Si se produjera una incidencia durante la ejecución del contrato que conllevara un acceso accidental o incidental a Datos Personales responsabilidad del encargado de tratamiento no contemplados, el adjudicatario deberá

ponerlo en conocimiento del encargado de tratamiento , en concreto de su Delegado de Protección de Datos, con la mayor diligencia y a más tardar en el plazo de 18 horas.

Santiago de Compostela,

Fdo.: Benigno Rosón Calvo Subdirector Xeral de Sistemas e Tecnoloxías da Información

Fdo.: Alberto Fuentes Losada Secretario Xeral Técnico

DIRECCIÓN XERAL DE RECURSOS ECONÓMICOS
SERVIZO GALEGO de SAÚDE
XUNTA DE GALICIA

A DIRECTORA XERAL DE RECURSOS ECONÓMICOS

Mª Jesús Piñeiro Bello

Documento firmado digitalmente por:
Fuentes Losada, Alberto: 28/12/2018 12:53
Rosón Calvo, Benigno: 28/12/2018 12:43

SAOC-Q4G4-BOAH-OFWB-Z815-4599-8023-041