

## ANEXO II

### 1 PROTECCIÓN DE DATOS

#### 1.1 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); la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y la normativa complementaria.

Dado que la contratación implica el acceso del contratista a datos de carácter personal de cuyo tratamiento es responsable la entidad contratante, aquél tendrá la consideración de encargado del tratamiento. El acceso a esos datos no se considerará comunicación de datos, según lo previsto en el artículo 28 del RGPD.

#### 1.2 TRATAMIENTO DE DATOS PERSONALES

Para el cumplimiento del objeto de esta licitación, el adjudicatario deberá tratar los datos personales de los cuales la Secretaría Xeral de la Consellería de Sanidade, en nombre del Sistema Sanitario Público de Galicia (en adelante Consellería de Sanidade) 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 Consellería de Sanidade 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 Consellería de Sanidade estuviese de

acuerdo con lo solicitado se generaría un contrato de tratamiento de datos actualizado, de modo que el mismo siempre recoja fielmente el detalle del tratamiento.

## 2 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 estipulaciones:

### 2.1.1 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 la Consellería de Sanidade por escrito en cada momento.

El adjudicatario informará inmediatamente a la Consellería de Sanidade cuando, en su opinión, una instrucción sea contraria a la normativa de protección de Datos Personales aplicable en cada momento.

### 2.1.2 Utilizar los datos personales objeto de tratamiento, o los que recoja para su inclusión, sólo para la finalidad objeto de este encargo. No utilizará ni aplicará los Datos Personales con una finalidad distinta a la ejecución del objeto del Contrato, y en ningún caso podrá utilizar los datos para fines propios.

### 2.1.3 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.

En particular, y sin carácter limitativo, se obliga a aplicar las medidas de protección del nivel de riesgo y seguridad detalladas en el sumario de tratamiento recogido en forma de tabla al final de este Anexo II (a partir de ahora, Sumario de Tratamiento)

### 2.1.4 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.



- 2.1.5 Llevar un listado de personas autorizadas para tratar los Datos Personales objeto de este pliego 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 Consellería de Sanidade dicha documentación acreditativa.

Para la gestión de permisos de accesos a sistemas de información bajo el control de la Consellería de Sanidade se seguirán las instrucciones que ella dicte.

- 2.1.6 Garantizar la formación necesaria en materia de protección de Datos Personales de las personas autorizadas a su tratamiento.
- 2.1.7 Salvo que cuente en cada caso con la autorización expresa del Responsable del Tratamiento, no comunicar (ceder) ni difundir los Datos Personales a terceros, ni siquiera para su conservación.
- 2.1.8 Debido a la naturaleza del tratamiento encargado, el adjudicatario debe nombrar Delegado de Protección de Datos, y comunicarlo a la AEPD, así como la identidad y datos de contacto de la(s) persona(s) física(s) designada(s) por el adjudicatario como sus representante(s) a efectos de protección de los Datos Personales (representantes del Encargado de Tratamiento), responsable(s) del cumplimiento de la regulación del tratamiento de Datos Personales, en las vertientes legales/formales y en las de seguridad.
- 2.1.9 Una vez finalizada la prestación contractual objeto del presente Pliego, se compromete, según corresponda y se instruya en el Sumario de Tratamiento, 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; al no existir permiso o requerimiento por ley o por norma de derecho comunitario para su conservación, por lo que se procederá a la destrucción. No obstante, y aportando justificación de dicha solicitud, el Encargado del Tratamiento podrá solicitar a la Consellería de Sanidade conservar los datos durante el tiempo que puedan derivarse responsabilidades de su relación con el Responsable del Tratamiento. En caso de ser aprobada esta solicitud, los Datos Personales se conservarán bloqueados y por el tiempo mínimo, destruyéndose de forma segura y definitiva al final de dicho plazo.**

- 2.1.10 Según corresponda y se indique en el Sumario de Tratamiento, a llevar a cabo el tratamiento de los Datos Personales en los sistemas / dispositivos de tratamiento, tanto manuales como automatizados, y en las ubicaciones que en el citado Sumario se especifican, equipamiento que podrá estar bajo el control de la Consellería de Sanidade o



bajo el control directo o indirecto del adjudicatario, u otros que hayan sido expresamente autorizados por escrito por la Consellería de Sanidade, según se establezca en dicho Sumario en su caso, y únicamente por los usuarios o perfiles de usuarios asignados a la ejecución del objeto de este Pliego.

- 2.1.11 Salvo que se indique otra cosa en el Sumario de Tratamiento o se instruya así expresamente por la Consellería de Sanidade, a 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 Pliego 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 a la Consellería de Sanidade de esa exigencia legal, con antelación suficiente a efectuar el tratamiento, y garantizará el cumplimiento de cualesquiera requisitos legales que sean aplicables a la Consellería de Sanidade, salvo que el Derecho aplicable lo prohíba por razones importantes de interés público.

- 2.1.12 De conformidad con el artículo 33 del RGPD, comunicar a la AEPD, de forma inmediata y a más tardar en el plazo de 72 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.

Se mantendrá en todo momento informada a la Consellería de Sanidade de las comunicaciones realizadas en este sentido.

- 2.1.13 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 a la Consellería de Sanidade 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, e incluyendo la identificación fehaciente de quien ejerce el derecho.



Asistirá a la Consellería de Sanidade, siempre que sea posible, para que ésta pueda cumplir y dar respuesta a los ejercicios de Derechos.

- 2.1.14 Colaborar con la Consellería de Sanidade 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.**

Asimismo, pondrá a disposición de la Consellería de Sanidade, a requerimiento de esta, toda la información necesaria para demostrar el cumplimiento de las obligaciones previstas en este Pliego y demás documentos contractuales y colaborará en la realización de auditoras e inspecciones llevadas a cabo, en su caso, por la AEPD.

- 2.1.15 En los casos en que la normativa así lo exija (ver art. 30.5 RGPD), llevar, por escrito, incluso en formato electrónico, y de conformidad con lo previsto en el artículo 30.2 del RGPD un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de la Consellería de Sanidade (Responsable del tratamiento), que contenga, al menos, las circunstancias a que se refiere dicho artículo.
- 2.1.16 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 de la Consellería de Sanidade a requerimiento de esta. Asimismo, durante la vigencia del contrato, pondrá a disposición de la Consellería de Sanidade toda información, certificaciones y auditorías realizadas en cada momento.
- 2.1.17 Derecho de información: El encargado del tratamiento, en el momento de la recogida de los datos, debe 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.

La presente cláusula 2.1 y las obligaciones en ella establecidas, así como el Sumario de Tratamiento constituyen el contrato de encargo de tratamiento entre la Consellería de Sanidade y el adjudicatario a que hace referencia el artículo 28.3 RGPD. Las obligaciones y prestaciones que aquí se contienen no son retribuíbles de forma distinta de lo previsto en el presente pliego y demás documentos contractuales y tendrán la misma duración que la





prestación de Servicio objeto de este pliego y su 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 pliego no se requiere que el adjudicatario acceda a ningún otro Dato Personal responsabilidad de la Consellería de Sanidade, y por tanto no está autorizado en caso alguno al acceso o tratamiento de otro dato, que no sean los especificados en el Sumario de Tratamiento. Si se produjera una incidencia durante la ejecución del contrato que conllevara un acceso accidental o incidental a Datos Personales responsabilidad de la Consellería de Sanidade no contemplados en el Sumario de Tratamiento el adjudicatario deberá ponerlo en conocimiento de la Consellería de Sanidade, en concreto de su Delegado de Protección de Datos, con la mayor diligencia y a más tardar en el plazo de 72 horas.

## 2.2 SUB-ENCARGOS DE TRATAMIENTO ASOCIADOS A SUBCONTRATACIONES

Dado que el pliego permite la subcontratación de actividades dentro de su objeto, y en caso de que el adjudicatario pretenda subcontratar con terceros la ejecución del contrato y el subcontratista, si fuera contratado, deba acceder a Datos Personales, el adjudicatario lo pondrá en conocimiento previo de la Consellería de Sanidade, identificando qué tratamiento de datos personales conlleva, para que la Consellería de Sanidade decida, en su caso, si otorgar o no su autorización a dicha subcontratación.

En todo caso, para autorizar la contratación, es requisito imprescindible que se cumplan las siguientes condiciones (si bien, aun cumpliéndose las mismas, corresponde a la Consellería de Sanidade 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 de la Consellería de Sanidade.
- 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 pliego, el cual será puesto a disposición de la Consellería de Sanidade a su mera solicitud para verificar su existencia y contenido.

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





## 2.3 INFORMACIÓN

Los datos de carácter personal vinculados a las ofertas presentadas por los licitadores serán tratados por la Consellería de Sanidade para ser incorporados al sistema de tratamiento “Gestión económica, presupuestaria y relaciones económicas con terceros”, cuya finalidad es, entre otras, la tramitación de los expedientes de contratación y gasto y la formalización, desarrollo y ejecución del contrato.

Finalidad necesaria para el cumplimiento de una obligación legal de la Consellería de Sanidade.

Los datos de carácter personal serán comunicados a entidades financieras, Agencias Tributaria autonómica y estatal, Consellería de Facenda, Ministerio de Hacienda, organismos de intervención autonómica y estatal, Consello de Contas, Tribunal de Cuentas y todos los posibles organismos y empresas que sean designados por la Comunidad Autónoma, el Gobierno de España y las instituciones y organismos de la Unión Europea en la auditoría de fondos FEDER. Estos datos también serán incluidos en las Plataforma de Contratación Autonómica y del Estado, así como en el Registro Público de Contratos. También podrán ser comunicados en base a la legislación de contratación del sector público y a la legislación de transparencia y acceso a la información pública.

Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad y del tratamiento de los datos, conforme a la Ley 58/2003, de 17 de diciembre, General Tributaria, además de los periodos establecidos en la normativa de archivos y patrimonio documental tanto autonómica como estatal.

Los derechos de acceso, rectificación, supresión y portabilidad de sus datos, de limitación y oposición a su tratamiento, así como a no ser objeto de decisiones basadas únicamente en el tratamiento automatizado de sus datos, cuando procedan, se pueden ejercitar ante la Secretaría Xeral Técnica de la Consellería de Sanidade, Edificio Administrativo San Lázaro, C/San Lázaro, s/n, 15703 – Santiago de Compostela o en la dirección de correo electrónico [dpd@sergas.gal](mailto:dpd@sergas.gal).



## SUMARIO DE TRATAMIENTO DE DATOS PERSONALES

### **Descripción general del tratamiento de Datos Personales a efectuar**

#### Descripción

El tratamiento consistirá en:

Prestación de un servicio de apoyo “in situ” para los usuarios de los sistemas de información y la prestación de un servicio de oficina de coordinación de toda la atención remota e “in situ” a usuarios basada en la función Service Desk de la biblioteca ITIL.

Todos los servicios se apoyarán en una metodología basada en la biblioteca ITIL v.3 (incorporada na Consellería de Sanidade co nome Xanela de Servizos T.I.).

El alcance de los trabajos se recoge detalladamente en el pliego de prescripciones técnicas.

La contratación se desagrega en los siguientes LOTES:

Lote 1: Apoyo usuarios zona norte

Lote 2: Apoyo usuarios zona sur

El lote 1 incluye la prestación en los centros de las provincias de Coruña y Lugo.

El Lote 2 incluye la prestación en los centros de las provincias de Ourense y Pontevedra.

### **Colectivos y Datos Tratados**

Los colectivos de interesados y Datos Personales tratados a las que puede tener acceso el adjudicatario son:

<b>Tratamientos/Ficheros principales colectivos y de interesados</b>	<b>Datos Personales del tratamiento/fichero a los que se puede acceder</b>
Gestión de historia Clínica y Actividad asistencial	<p>Los datos personales a tratar son:</p> <ul style="list-style-type: none"> <li>• Categorías especiales de datos (datos sensibles): origen racial, religión, salud y vida sexual</li> <li>• Datos de carácter identificativo</li> <li>• Datos de características personales</li> <li>• Datos de circunstancias sociales</li> <li>• Datos académicos y profesionales</li> <li>• Datos de detalle de empleo y carrera administrativos</li> </ul>





<b>Tratamientos/Ficheros principales colectivos y de interesados</b>	<b>Datos Personales del tratamiento/fichero a los que se puede acceder</b>
Identificación usuarios y profesionales del sistema público sanitario	Los datos personales a tratar son: • Datos de carácter identificativo • Datos académicos y profesionales
Gestión de incidencias y peticiones de Tecnologías de la Información y brechas de seguridad	Los datos personales a tratar son: • Datos identificativos • Categorías especiales de datos: aquellos necesarios para la resolución de la incidencia.
Formación	Los datos personales a tratar son: • Datos de carácter identificativo • Datos académicos y profesionales

### **Elementos del tratamiento**

El tratamiento de los Datos Personales comprenderá:

<input type="checkbox"/> Recogida (captura de datos)	<input type="checkbox"/> Registro (grabación)	<input checked="" type="checkbox"/> Estructuración	<input type="checkbox"/> Modificación
<input type="checkbox"/> Conservación (almacenamiento)	<input checked="" type="checkbox"/> Extracción (retrieval)	<input checked="" type="checkbox"/> Consulta	<input type="checkbox"/> Cesión
<input type="checkbox"/> Difusión	<input checked="" type="checkbox"/> Interconexión (cruce)	<input checked="" type="checkbox"/> Cotejo	<input type="checkbox"/> Limitación
<input type="checkbox"/> Supresión	<input type="checkbox"/> Destrucción (de copias temporales)	<input type="checkbox"/> Conservación (en sus sistemas de información)	<input type="checkbox"/> Otros: _____
<input type="checkbox"/> Duplicado	<input checked="" type="checkbox"/> Copia (copias temporales)	<input type="checkbox"/> Copia de seguridad	<input checked="" type="checkbox"/> Recuperación

Una vez finalice el encargo, el adjudicatario debe:

- a) Devolver al responsable del tratamiento los datos de carácter personal y, si procede, los soportes donde consten, una vez cumplida la prestación. La devolución debe comportar el borrado total de los datos existentes en los equipos informáticos utilizados por el encargado.

Además, el Responsable del Tratamiento podrá requerir al encargado para que en vez de la opción a), cumpla con la b) o con la c) siguientes:



- b) Devolver al encargado que designe por escrito el responsable del tratamiento, los datos de carácter personal y, si procede, los soportes donde consten, una vez cumplida prestación. La devolución debe comportar el borrado total de los datos existentes en los equipos informáticos utilizados por el encargado. No obstante, el encargado puede conservar una copia, con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.
- c) Destruir los datos, una vez cumplida la prestación. Una vez destruidos, el encargado debe certificar su destrucción por escrito y debe entregar el certificado al responsable del tratamiento.

En cualquiera de los 3 casos, y aportando justificación de dicha solicitud, el Encargado del Tratamiento podrá solicitar a la Consellería de Sanidade conservar los datos durante el tiempo que puedan derivarse responsabilidades de su relación con el Responsable del Tratamiento o de la ejecución de la prestación. En caso de ser aprobada esta solicitud, los Datos Personales se conservarán bloqueados y por el tiempo mínimo, destruyéndose de forma segura y definitiva al final de dicho plazo.

### ***Medidas de seguridad***

Los datos deben protegerse empleando las medidas que un empresario ordenado debe tomar para evitar que dichos datos pierdan su razonable confidencialidad, integridad y disponibilidad. De acuerdo con la evaluación de riesgos realizada, se deben implantar, al menos, las medidas de seguridad siguientes:

- Formatear los soportes de datos cuando vayan a ser dedicados a otro uso, desechados o reubicados, garantizando la completa eliminación de cualquier información previamente existente.
- Instalar, configurar y manipular los equipos siguiendo las instrucciones dadas por la Consellería de Sanidade y las recomendaciones de seguridad vigentes en cada momento. En caso que las instrucciones entrasen en contradicción con recomendaciones de fabricantes, lo pondrá en conocimiento de la Consellería de Sanidade.
- Tratar los datos siguiendo las instrucciones dadas por la Consellería de Sanidade y las recomendaciones de seguridad vigentes en cada momento. En caso que las instrucciones entrasen en contradicción con metodologías, recomendaciones o estándares de seguridad, lo pondrá en conocimiento de la Consellería de Sanidade.
- Formar y supervisar a su personal de manera continua para garantizar el máximo rigor en el tratamiento de los datos, en especial en todos los aspectos relativos al aseguramiento de su calidad y a la seguridad de la información.
- El personal del adjudicatario, en caso de tener acceso a las sesiones abiertas por usuarios a los que esté dando apoyo, debe limitar el uso de los dispositivos de entrada y salida a aquellos



casos imprescindibles, manteniendo siempre informado al usuario de la finalidad de las operaciones que realice.

- Ejecutar su trabajo con pleno respeto a la actividad asistencial de los centros en que se realiza, garantizando la intimidad de los pacientes.

Así como cualquier otra medida que el adjudicatario pueda identificar y proponer

El adjudicatario no podrá no implementar o suprimir dichas medidas mediante el empleo de un análisis de riesgo o evaluación de impacto salvo aprobación expresa de la Consellería de Sanidade.

A estos efectos, el personal del adjudicatario debe seguir las medidas de seguridad establecidas por la Consellería de Sanidade, no pudiendo efectuar tratamientos distintos de los definidos por la Consellería de Sanidade.

Santiago de Compostela,

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

O Secretario Xeral Técnico. Alberto Fuentes Losada

