ANEXO II. ACUERDO DE ENCARGADO DE TRATAMIENTO DE DATOS

1. OBLIGACIONES GENERALES

Estas obligaciones generales y las establecidas en el apartado 2 de este acuerdo relativo al Tratamiento de Datos Personales constituyen el contrato de encargado de tratamiento a que hace referencia el artículo 28.3 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 el 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, en adelante RGPD) entre el Servicio Andaluz de Salud (SAS) como responsable y la persona adjudicataria como encargado del tratamiento.

De conformidad con lo previsto en el artículo 28 del RGPD, la persona adjudicataria se obliga a garantizar el cumplimiento de las siguientes obligaciones, complementadas y concretadas con lo detallado en el apartado 2. Tratamiento de Datos Personales:

a) Tratar los Datos Personales conforme a las instrucciones documentadas en el presente Pliego o demás documentos contractuales aplicables a la ejecución del contrato y aquellas que, en su caso, reciba del SAS por escrito en cada momento; salvo que esté obligado a ello en virtud del Derecho de la Unión Europea o nacional que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público.

b) No utilizar ni aplicar los Datos Personales con una finalidad distinta a la ejecución del objeto del Contrato.

c) 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.

El uso de aplicaciones y sistemas del SAS por parte de la persona adjudicataria contemplará el Código de Conducta en el uso de las Tecnologías de la Información y la Comunicación para profesionales públicos de la Administración de la Junta de Andalucía, aprobado por Resolución de 22 de octubre de 2020, de la Secretaría General para la Administración Pública.

En particular, y sin carácter limitativo, se obliga a aplicar las medidas de protección del nivel de riesgo y seguridad detallados en el apartado 2 de este documento.

d) 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 de la persona adjudicataria, siendo deber de la persona adjudicataria instruir a las personas que de ella 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.

e) 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 del SAS dicha documentación acreditativa.

f) Garantizar la formación necesaria en materia de protección de Datos Personales de las personas autorizadas a su tratamiento.

g) 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.

h) Nombrar Delegado de Protección de Datos, en caso de que sea necesario según el RGPD, y comunicarlo al SAS, también cuando la designación sea voluntaria, así como la identidad y datos de contacto de la(s) persona(s) física(s) designada(s) por la persona adjudicataria 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.

i) Una vez finalizada la prestación contractual objeto del presente Pliego, se compromete, según corresponda y se instruya en el apartado 2 de este documento, a devolver o destruir (i) los Datos Personales a los que haya tenido acceso; (ii) los Datos Personales generados por la persona adjudicataria 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.

j) Según corresponda y se indique el apartado 2 de este documento, a 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 citado Anexo se especifican, equipamiento que podrá estar bajo el control del SAS o bajo el control directo o indirecto de la persona adjudicataria, u otros que hayan sido expresamente autorizados por escrito por el SAS, según se establezca en dicho Anexo en su caso, y únicamente por los usuarios o perfiles de usuarios asignados a la ejecución del objeto de este Pliego.

k) 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 acuerdo 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, que se indique otra instrucción en el apartado 2 de este acuerdo o se instruya así expresamente por el SAS.

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

l) De conformidad con el artículo 33 RGPD, comunicar al SAS, de forma inmediata y en un **plazo máximo de 24 horas**, desde que tuvo conocimiento de la misma, cualquier brecha de la seguridad de los datos personales a su cargo, conjuntamente 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.

La notificación de brechas de la seguridad de los datos se realizará obligatoriamente a través del Service Desk (AyudaDigital/MiCentroServicios, teléfono 955017000) del CGES Centro de Gestión de Servicios TIC, enviando copia del comunicado por correo electrónico al Delegado de Protección de Datos (DPD) del SAS dpd.sspa@juntadeandalucia.es, así como a ustic.stic.sspa@juntadeandalucia.es.

m) 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 SAS 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.

La persona adjudicataria asistirá al SAS, siempre que sea posible, para que ésta pueda cumplir y dar respuesta a los ejercicios de Derechos.

n) Colaborar con el SAS 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 del SAS, a requerimiento de éste, 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 auditorías e inspecciones llevadas a cabo, en su caso, por el SAS.

o) 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 del SAS, que contenga, al menos, las circunstancias a que se refiere dicho artículo.

p) 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 SAS a requerimiento de este. Asimismo, durante la vigencia del contrato, pondrá a disposición del SAS toda información, certificaciones y auditorías realizadas en cada momento.

q) 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.

2. TRATAMIENTO DE DATOS PERSONALES

A) Descripción general del tratamiento de Datos Personales a efectuar

El tratamiento consistirá en: Gestión de Sistemas Automáticos de Dispensación de Medicamentos (SADME) en el Hospital Universitario Reina Sofía, que permita el almacenamiento, dispensación, de manera controlada electrónicamente e integrado en el sistema de información del hospital.

El personal adscrito por la persona adjudicataria, para proporcionar las prestaciones establecidos en el presente pliego puede tratar Datos Personales. Los Datos Personales se tratarán únicamente por el personal adscrito y al único fin de efectuar el alcance contratado.

B) Colectivos y Datos Tratados

Los colectivos de interesados y Datos Personales tratados a las que puede tener acceso la persona adjudicataria son:

Tratamientos de datos	**Principales colectivos de interesados**	**Datos Personales del tratamiento a los que se puede acceder**	**Ubicación y control**
Gestión SADME	Pacientes	Datos administrativos. Datos de prescripción electrónica.	Sistema de información para gestión del SADME y conectividad a la Historia Digital de Salud del Ciudadano. CPD del Hospital Universitario Reina Sofía de Córdoba - SAS Sistema bajo control indirecto por la persona adjudicataria.

Gestión SADME	Profesionales	Datos administrativos.	(Idem)
Tratamiento N: (explicitar)	*Categorías de interesados (por ejemplo, ciudadanía, profesional, etc...)*	_____	_____

C) Elementos del tratamiento

El tratamiento de los Datos Personales comprenderá: *(márquese lo que proceda)*:

☐ Recogida (captura de datos) ☐ Registro (grabación) ☐ Estructuración

☐ Modificación ☐ Conservación (almacenamiento) ☐ Extracción (retrieval)

☐ Consulta ☐ Cesión ☐ Difusión

☐ Interconexión (cruce) ☐ Cotejo ☐ Limitación

☐ Supresión ☐ Destrucción (de copias temporales) ☐ Conservación (en sus sistemas de información)

☐ Duplicado ☐ Copia (copias temporales) ☐ Copia de Seguridad

☐ Recuperación

☐ Otros (especificar)

D) Disposición de los datos al terminar la prestación

Una vez finalice el encargo, la persona adjudicataria 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. No obstante, el encargado puede conservar una copia, con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

No obstante, 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) Entregar 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 entrega 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. No obstante, el encargado puede conservar una copia, con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

E) 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 el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), las medidas de seguridad a implantar serán las determinadas por los preceptivos análisis de riesgos y, si procede, evaluación de impacto en la protección de datos, que serán realizados por el órgano de contratación **previo al despliegue del sistema**.

Las medidas deberán corresponder con lo establecido en el **Anexo II del ENS**, en función de los activos presentes en el sistema de información y las dimensiones de seguridad relevantes, considerando que el sistema, conforme a los criterios establecidos en el anexo I del ENS, como mínimo, es de **categoría MEDIA**.

La persona adjudicataria deberá documentar la relación de medidas de seguridad aplicables en base a la categoría del sistema, prestando especial atención a:

[mp.sw] Medidas de Protección de las aplicaciones informáticas.

[mp.sw.2] Aceptación y puesta en servicio

1. *Antes de pasar a producción se comprobará el correcto funcionamiento de la aplicación. Se verificará que:*

    a) *Se cumplen los criterios de aceptación en materia de seguridad.*

b) *No se deteriora la seguridad de otros componentes del servicio.*

2. *Las pruebas se realizarán en un entorno aislado (pre-producción).*

[mp.s.2] Protección de servicios y aplicaciones web.

- Cuando la información requiera control de acceso se garantizará la imposibilidad de acceder a la información obviando la autenticación, en particular, tomando medidas en los siguientes aspectos:

a) Se evitará que el servidor ofrezca acceso a los documentos por vías alternativas al protocolo determinado.

b) Se prevendrán ataques de manipulación del localizador uniforme de recursos (Uniform Resource Locator, URL).

c) Se prevendrán ataques de manipulación de fragmentos de información que se almacena en el disco duro del visitante de una página web a través de su navegador, a petición del servidor de la página, conocido en terminología inglesa como cookies.

d) Se prevendrán ataques de inyección de código.

– Se prevendrán intentos de escalado de privilegios.

– Se prevendrán ataques de cross site scripting.

- Auditorías de seguridad.

- Se realizarán auditorías continuas de seguridad de «caja negra» sobre las aplicaciones web durante la fase de desarrollo y antes de la fase de producción. La frecuencia de estas auditorías de seguridad quedará definida en el procedimiento de auditoría.

- Como alternativa, se podrán realizar auditorías de seguridad de «caja blanca» sobre las aplicaciones web durante la fase de desarrollo.

Se emplearán metodologías definidas y herramientas automáticas de detección de vulnerabilidades en la realización de las auditorías de seguridad sobre las aplicaciones web.

Una vez finalizada una auditoría de seguridad, se analizarán los resultados y se solventarán las vulnerabilidades encontradas mediante los procedimientos definidos [op.exp.5].

En todo caso, los mecanismos concretos para:

a. Garantizar la confidencialidad, integridad, disponibilidad, trazabilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
b. Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
c. Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.
d. Seudonimizar y cifrar los datos personales, en su caso.

La persona adjudicataria no podrá no implementar o suprimir dichas medidas mediante el empleo de un análisis de riesgo o evaluación de impacto salvo aprobación expresa del órgano de contratación.

A estos efectos, el personal de la persona adjudicataria debe seguir las medidas de seguridad establecidas en el pliego de prescripciones técnicas y en su caso cualesquiera otras indicadas por el órgano de contratación, no pudiendo efectuar tratamientos distintos de los definidos.

F) Sub-encargos de tratamiento asociados a subcontrataciones

Cuando se produzca una subcontratación con terceros de la ejecución del contrato y el subcontratista deba acceder a Datos Personales, la persona adjudicataria lo pondrá en conocimiento previo del SAS, identificando qué tratamiento de datos personales conlleva, para que este decida, en su caso, si otorgar o no su autorización a dicha subcontratación. El silencio del SAS es en todo caso negativo.

En todo caso, para su autorización es requisito que se cumplan las siguientes condiciones:

- Que el tratamiento de datos personales por parte de la persona subcontratista se ajuste a la legalidad vigente, lo contemplado en este pliego y a las instrucciones del órgano de contratación.
- Que la persona adjudicataria 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 del órgano de contratación.

La persona adjudicataria informará al órgano de contratación de cualquier cambio previsto en la incorporación o sustitución de otras personas subcontratistas, dando así la oportunidad de otorgar el consentimiento previsto en esta cláusula. La no respuesta a dicha solicitud equivale a oponerse a dichos cambios.

G) Información sobre tratamiento de datos personales contenidos en el contrato y los necesarios para su tramitación

Los datos de carácter personal contenidos en el contrato y los necesarios para su gestión serán tratados por el órgano de contratación con la finalidad de llevar a cabo la gestión presupuestaria y económica del mismo, siendo la persona responsable del tratamiento la que así esté designada formalmente en el ámbito de la entidad.

La base jurídica del tratamiento es el cumplimiento de una obligación legal de un fin de interés público y el ejercicio de poderes públicos conferidos a la persona responsable del tratamiento por la Ley de Contratos del Sector Público (LCSP), el Texto Refundido de la Ley General de la Hacienda Pública de la Junta de Andalucía y demás que regule los gastos públicos.

No se prevé la comunicación de datos de carácter personal a terceras personas, salvo las impuestas por el ordenamiento jurídico. Los datos se conservarán por el tiempo que exija la normativa sobre contratación pública, hacienda pública y archivo con fines de interés público.

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 el órgano de contratación.

Puede ejercer estos derechos mediante una solicitud dirigida a la persona responsable del tratamiento, preferentemente a través del formulario para el ejercicio de estos derechos disponible en www.juntadeandalucia.es/servicioandaluzdesalud/protecciondedatos. Además, puede solicitar el ejercicio de sus derechos solicitándolo por cualquiera de los medios para presentación de solicitudes y en cualquiera de los registros conformes con la Ley 39/2015.

H) Documentación a presentar

La persona adjudicataria deberá presentar la información correspondiente a este apartado, en relación a los colectivos y datos tratados, elementos del tratamiento, medidas de seguridad a implementar, así como los datos de contacto para el tratamiento.

En cumplimiento del artículo 13 del ENS, la persona adjudicataria deberá designar un POC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado, que cuente con el apoyo de los órganos de dirección, y que canalice y supervise, tanto el cumplimiento de los requisitos de seguridad como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio.

Dicho POC de seguridad será el propio responsable de seguridad de la persona adjudicataria, formará parte de su área o tendrá comunicación directa con la misma. Su identificación será comunicada por el órgano de contratación a su Responsable de Seguridad TIC para su inclusión en el registro de POC de seguridad de proveedores y comunicación al Centro de respuesta a incidentes de Ciberseguridad de referencia, Andalucía CERT.

-POC de seguridad: *<Datos de contacto>*

-Delegado de protección de datos (DPD) *<Datos de contacto>*
(si procede)

Si la persona adjudicataria tiene previsto subcontratar servicios asociados al contrato con acceso a datos personales, la/s persona/s empresaria/s serían:

Tratamiento N _____ Perfil empresarial 1 _____

Tratamiento N _____ Perfil empresarial 2 _____

Tratamiento N _____ Perfil empresarial 3 _____

Cualquier cambio que se produzca a lo largo de la vida del contrato de la información facilitada será comunicado de forma inmediata al responsable, dirigiéndose además por correo electrónico al DPD del SAS dpd.sspa@juntadeandalucia.es, así como a us-tic.stic.sspa@juntadeandalucia.es.