ANEXO II: Requerimientos de protección de datos

SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN

1.1 Normativa de seguridad.

Considerando lo dispuesto en el artículo 2 del *Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad* (***ENS***), donde se describe la obligación de exigir a las entidades del sector privado que presten servicios o provean soluciones a las entidades públicas, de conformidad con el Esquema Nacional de Seguridad, la ENTIDAD CONTRATANTE, considera necesario que ENTIDAD LICITADORA, esté en condiciones de exhibir la correspondiente Declaración o Certificación de Conformidad con el Esquema Nacional de Seguridad, para la categoría de seguridad de que se trate, de los sistemas que intervengan en la prestación de los servicios indicados, así como mantener la conformidad vigente durante la vigencia del contrato.

En el supuesto de que el adjudicatario no pudiera mantener la conformidad con el ENS -por pérdida, retirada o suspensión de la Certificación de Conformidad o imposibilidad de mantener la Declaración de Conformidad-, deberá comunicar esta circunstancia, de forma inmediata y sin dilación indebida, a la ENTIDAD CONTRATANTE, quien considerará el impacto en la prestación objeto del contrato de dicha circunstancia.

La ENTIDAD ADJUDICATARIA asume su obligación de cumplir plenamente con el Esquema Nacional de Seguridad.

Adicionalmente, la ENTIDAD 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 del servicio que presta o solución que provea, 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 organización contratada, formará parte de su área o tendrá comunicación directa con la misma.

1.2 Normativa de protección de datos.

En el caso de que el Adjudicatario, en el ejercicio de la prestación del servicio, tuviera que tratar con datos personales del HOSPITAL GENERAL UNIVERSITARIO GREGORIO MARAÑÓN por razón de la prestación del servicio, cumplirá con la legislación vigente en materia de protección de datos personales que resulte de aplicación, en concreto con la *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales* (***LOPDGDD***), y 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 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)* (***RGPD***); o cualesquiera otras aplicables en materia de Protección de Datos que se encuentren en vigor a la adjudicación de este contrato o que puedan estarlo durante su vigencia.

Así, y a los efectos de este contrato, el Hospital Universitario Gregorio Marañón (en adelante, HGUGM), tendrá la consideración de Responsable del tratamiento y el Adjudicatario tendrá la

Dr. Esquerdo, 46
28007 – Madrid
Web: www.madrid.org/hospitalgregoriomaranon

consideración de Encargado del Tratamiento conforme a lo establecido en los artículos 28 y 29 del RGPD, así como en el artículo 33 de la LOPDGDD.

1.3 Encargado del Tratamiento.

El Adjudicatario, se compromete a cumplir las medidas y requisitos de seguridad exigidos por el HGUGM.

El tratamiento de datos personales por el Adjudicatario, se regirá por un contrato, Pliego o acto jurídico análogo, donde se establezca el objeto, la duración, la naturaleza y finalidad del tratamiento, así como el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable.

Las obligaciones derivadas de ésta responsabilidad asumida por el Adjudicatario, serán recogidas en un documento específico que será firmado por el HGUGM y el Adjudicatario de forma previa al inicio de los trabajos.

1.4 Encargado del Tratamiento.

El Encargado del Tratamiento se compromete a cumplir las medidas y requisitos de seguridad exigidos por el HGUGM. El coste de las actuaciones de cualquier tipo, derivadas del cumplimiento de RGPD y normativa relacionada, serán por cuenta del Encargado del Tratamiento.

El tratamiento de datos personales por el Encargado del Tratamiento, se regirá por un contrato o acto jurídico análogo, donde se establezca el objeto, la duración, la naturaleza y finalidad del tratamiento, así como el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable.

Las obligaciones derivadas de ésta responsabilidad asumida por el Encargado del Tratamiento, serán recogidas en un documento específico que será firmado por el HGUGM y el Encargado del Tratamiento de forma previa al inicio de los trabajos.

1.5 Limitación del acceso o tratamiento.

El Adjudicatario limitará el acceso o tratamiento de datos personales pertenecientes al HGUGM limitándose a realizar el citado acceso o tratamiento cuando se requiera imprescindiblemente para la prestación del servicio y/o de las obligaciones contraídas, y en todo caso limitándose a los datos que resulten estrictamente necesarios.

1.6 Instrucciones de Tratamiento.

Toda la información que se entregue al adjudicatario para el desarrollo de los trabajos tendrá el carácter de confidencial.

A los efectos de la prestación del servicio por parte del Adjudicatario, en su calidad de Encargado del Tratamiento quedará obligado, a mantener absoluta confidencialidad y reserva sobre cualquier dato que pudiera conocer con ocasión del cumplimiento o realización de los trabajos objeto de este pliego, especialmente los personales o empresariales, que no podrá copiar o utilizar con fin distinto al que figura en este pliego, ni tampoco ceder a otros ni siquiera a efectos de conservación.

Dr. Esquerdo, 46
28007 – Madrid
Web: www.madrid.org/hospitalgregoriomaranon

El adjudicatario quedará obligado además de por el deber de confidencialidad, por del deber de seguridad de los datos personales, en todas aquellas previsiones que estén contempladas en las actividades que formen parte del servicio adjudicado, en especial: El Encargado del Tratamiento, mediante la suscripción del contrato de adjudicación, asumirá el cumplimiento de lo previsto en las presentes cláusulas, atendiendo en especial, a los artículos 28, 29, 30 y 32 del RGPD:

- El Adjudicatario y el personal encargado de la realización de las tareas guardarán y asegurarán la confidencialidad, disponibilidad e integridad sobre todas las informaciones, documentos y asuntos a los que tengan acceso o conocimiento durante la vigencia del contrato, no revelando, transfiriendo o cediendo, ya sea verbalmente o por escrito, a cuantos datos conozcan como consecuencia de la prestación del servicio sanitario, sin límite temporal alguno.
- El Adjudicatario, mediante la suscripción del contrato de adjudicación, asumirá el cumplimiento de lo previsto en las presentes cláusulas, atendiendo en especial, a los artículos 28, 29, 30 y 32 del RGPD, así como los artículos 28 y 31 de la LOPDGDD.
- El Adjudicatario utilizará los datos personales única y exclusivamente, en el marco y para las finalidades determinadas en el objeto del servicio adjudicado y del presente documento, y bajo las instrucciones del Responsable del Tratamiento, para aquellos aspectos relacionados con sus competencias.
- Accederá a los datos personales responsabilidad del Responsable del Tratamiento únicamente cuando sea imprescindible para el buen desarrollo de los servicios para los que ha sido contratado.
- En caso de que el tratamiento incluya la recogida de datos personales en nombre y por cuenta del Responsable del Tratamiento, el Adjudicatario deberá seguir los procedimientos e instrucciones que reciba del Responsable del Tratamiento, especialmente en lo relativo al deber de información y, en su caso, la obtención del consentimiento de los afectados.
- Si el Adjudicatario considera que alguna de las instrucciones del Responsable del Tratamiento infringe el RGPD, la LOPDGDD, o cualquier otra disposición en materia de protección de datos de la Unión o de los Estados miembros, informará inmediatamente al Responsable del Tratamiento.
- En caso de estar obligado a ello por el artículo 30 del RGPD y 31 de la LOPDGDD, el Adjudicatario mantendrá un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del Responsable del Tratamiento, que contenga la información exigida por el artículo 30.2 del RGPD.
- Dará apoyo al Responsable del Tratamiento en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando proceda.
- Dará apoyo al Responsable del Tratamiento en la realización de las consultas previas a la Autoridad de Control, cuando proceda.
- Pondrá a disposición del Responsable del Tratamiento toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen al Responsable del Tratamiento u otro auditor autorizado por este.
- En caso de estar obligado a ello por el artículo 37.1 del RGPD y por el artículo 34 de la LOPDGDD, designará un delegado de protección de datos y comunicará su identidad y datos de contacto al Responsable del Tratamiento, cumpliendo con todo lo dispuesto en los artículos 37, 38 y 39 del RGPD y 35 a 37 de la LOPDGDD.
- En caso de que el Adjudicatario deba transferir o permitir acceso a datos personales responsabilidad del Responsable del Tratamiento a un tercero en virtud del Derecho de la Unión o de los Estados miembros que le sea aplicable, informará al Responsable del

Dr. Esquerdo, 46
28007 – Madrid
Web: www.madrid.org/hospitalgregoriomaranon

Tratamiento de esa exigencia legal de manera previa, salvo que estuviese prohibido por razones de interés público.

- Se prohíbe el tratamiento de datos por terceras entidades que se encuentren en terceros países sin un nivel de protección equiparable al otorgado por la normativa de protección de datos personales vigente en España, salvo que se obtenga la preceptiva autorización de la Agencia Española de Protección de Datos para transferencias internacionales de datos, de conformidad con los artículos 44, 45, 46, 47, 48, y 49 del RGPD y los artículos 40, 41, 42 y 43 de la LOPDGDD.
- El Adjudicatario comunicará y hará cumplir a sus empleados, y a cualquier persona con acceso a los datos personales, las obligaciones establecidas en los apartados anteriores, especialmente las relativas al deber de secreto y medidas de seguridad.
- El Adjudicatario no podrá realizar copias, volcados o cualesquiera otras operaciones de conservación de datos, con finalidades distintas de las establecidas en el servicio adjudicado, sobre los datos personales a los que pueda tener acceso en su condición de Adjudicatario, salvo autorización expresa y por escrito del Responsable del Tratamiento.
- Adoptar y aplicar las medidas de seguridad estipuladas en el presente contrato, conforme lo previsto en el artículo 32 del RGPD, y el Esquema Nacional de Seguridad que resulte de aplicación, que garanticen la seguridad de los datos personales responsabilidad del Responsable del Tratamiento y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural.
- El Adjudicatario se compromete a formar e informar a su personal en las obligaciones que de tales normas dimanan, para lo cual programará las acciones formativas necesarias, incluida la formación en protección de datos y seguridad. Así mismo, el del Adjudicatario y su personal tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.
- El Adjudicatario comunicará al Responsable del Tratamiento, para aquellos aspectos relacionados con sus competencias, de forma inmediata, cualquier incidencia en los sistemas de tratamiento y gestión de la información que haya tenido o pueda tener como consecuencia la alteración, la pérdida o el acceso a datos personales, o la puesta en conocimiento por parte de terceros no autorizados de información confidencial obtenida durante la prestación del servicio.
- El Adjudicatario estará sujeto a las mismas condiciones y obligaciones descritas previamente en el presente documento, con respecto al acceso y tratamiento de cualesquiera documentos, datos, normas y procedimientos pertenecientes al Responsable del Tratamiento a los que pueda tener acceso en el transcurso de la prestación del servicio.
- Los diseños y desarrollos de software deberán, observar con carácter general, la normativa de seguridad de la información y de protección de datos de la Comunidad de Madrid y:
    - En todo caso observarán los requerimientos relativos a la identificación y autenticación de usuarios, estableciendo un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado, limitando la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

Dr. Esquerdo, 46
28007 – Madrid
Web: www.madrid.org/hospitalgregoriomaranon

- En ningún caso el equipo prestador del servicio objeto del contrato tendrá acceso ni realizará tratamiento de datos personales contenidos o soportados en los equipos o recursos mantenidos.

1.7 Destino de los datos al finalizar la prestación del servicio.

Una vez cumplida o resuelta la relación contractual acordada entre el Responsable del Tratamiento y el Adjudicatario, el Adjudicatario deberá solicitar al Responsable del Tratamiento instrucciones precisas sobre el destino de los datos personales de su responsabilidad, pudiendo elegir éste último entre su devolución, remisión a otro prestador de servicios o destrucción íntegra, siempre que no exista previsión legal que exija la conservación de los datos, en cuyo caso no podrá procederse a su destrucción. La devolución o destrucción de la información no eximirá al adjudicatario del cumplimiento de confidencialidad aquí reflejado.

Así mismo, el Responsable del Tratamiento tendrá derecho a exigir en cualquier momento que la información confidencial, proporcionada al adjudicatario, sea destruida o devuelta, ya sea antes, durante o después de la celebración.

1.8 Cesión o comunicación de datos a terceros.

El Adjudicatario no comunicará los datos accedidos o tratados a terceros, ni siquiera para su conservación. Así, el Adjudicatario no podrá subcontratar ninguna de las prestaciones que formen parte del objeto del pliego y que comporten el tratamiento de datos personales, salvo los servicios auxiliares necesarios para el normal funcionamiento de los servicios.

- En caso de que el Adjudicatario necesitara subcontratar todo o parte de los servicios contratados por el Responsable del Tratamiento en los que intervenga el tratamiento de datos personales, deberá comunicarlo previamente y por escrito al Responsable del Tratamiento, con una antelación de 1 mes, indicando los tratamientos que se pretende subcontratar e identificando de forma clara e inequívoca la empresa subencargada, así como sus datos de contacto. La subcontratación podrá llevarse a cabo si el Responsable del Tratamiento no manifiesta su oposición en el plazo establecido.
- El subencargado, también está obligado a cumplir las obligaciones establecidas en este documento para el Adjudicatario y las instrucciones que dicte el Responsable del Tratamiento.
- Corresponde al Adjudicatario exigir por contrato al subencargado el cumplimiento de las mismas obligaciones asumidas por él a través del presente documento.
- El Adjudicatario seguirá siendo plenamente responsable ante el Responsable del Tratamiento en lo referente al cumplimiento de las obligaciones.

1.9 Deber de información mutuo.

Las partes informan a los representantes que firman el presente contrato de que sus datos personales, van a ser tratados con la finalidad del mantenimiento de las relaciones contractuales de cada una de las partes, siendo imprescindible para ello que se aporten sus datos identificativos, el cargo que ostentan, número de DNI o documento equivalente y su firma.

Asimismo, las partes garantizan cumplir con el deber de información con respecto a sus empleados cuyos datos personales sean comunicados entre las partes para el mantenimiento y cumplimiento de la relación contractual. Las partes se comunicarán mutuamente la identidad de sus Delegados de Protección de Datos, en caso de que dicho nombramiento les sea de aplicación.

Dr. Esquerdo, 46
28007 – Madrid
Web: www.madrid.org/hospitalgregoriomaranon

La base jurídica que legitima el tratamiento de los datos de los interesados es la necesidad para la celebración y ejecución del presente contrato.

Los datos serán conservados durante la vigencia del presente contrato y, posteriormente, durante los años necesarios para atender las posibles responsabilidades derivadas de la relación contractual.

En todo caso, los afectados podrán ejercer sus derechos de acceso, rectificación, supresión y oposición, limitación, portabilidad ante la parte que corresponda a través de comunicación por escrito al domicilio social que consta al comienzo del presente documento, aportando fotocopia de su DNI o documento equivalente e identificando el derecho que se solicita. Asimismo, en caso de considerar vulnerado su derecho a la protección de datos personales, podrán interponer una reclamación ante la Agencia Española de Protección de Datos.

1.10 Responsabilidad en caso de incumplimiento.

En el caso de que el *adjudicatario* destinase los datos a otra finalidad, los comunicase o bien, los utilizase incumpliendo las estipulaciones contenidas en el presente pliego, o en general, los utilice de forma irregular, así como cuando no adoptase las medidas correspondientes para el almacenamiento y custodia de los mismos, será considerado también *responsable del tratamiento*, respondiendo de las infracciones en que hubiera incurrido personalmente. A tal efecto, se obliga a indemnizar al *Responsable del tratamiento,* por cualesquiera daños y perjuicios que sufra directamente, o por toda reclamación, acción o procedimiento, que traiga su causa de un incumplimiento o cumplimiento defectuoso por parte del *encargado del tratamiento* de lo dispuesto tanto en los Pliegos, como en lo dispuesto en la normativa reguladora de la protección de datos personales.

Dr. Esquerdo, 46
28007 – Madrid
Web: www.madrid.org/hospitalgregoriomaranon