METODOLOGÍA PARA EVALUACIÓN DE PRESTADORES DE SERVICIOS CON ACCESO A DATOS PERSONALES

Cautelas de privacidad en la selección de encargados de tratamiento de la Universidad de Huelva

Descripción breve

Recomendaciones del DPD para el cumplimiento de la normativa sobre protección de datos en el proceso de valorar y aprobar a los distintos prestadores de servicios que deban tener acceso a datos de carácter personal responsabilidad de la Universidad de Huelva en el desarrollo de las operaciones que se les encarguen.

Contenido

Introducción

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 (RGPD), ha supuesto un cambio total de paradigma a la hora de determinar y regular el cumplimiento de las obligaciones en materia de protección de datos, estableciendo la obligación legal, tanto para empresas privadas como para las Administraciones Públicas, de adoptar un enfoque de riesgos frente a los viejos modelos de cumplimiento meramente formal.

El art. 5.2. RGPD recoge el principio básico de la "responsabilidad proactiva" o "accountabilty", tradicionalmente conocido también como "obligación de diligencia debida"; indicando que

> ***"El responsable del tratamiento será responsable del cumplimiento (…) y capaz de demostrarlo".***

Ello obliga a las organizaciones a que sean ellas mismas quienes determinen y evalúen cuáles van a ser las mejores medidas que les permitan cumplir con la normativa y poder demostrarlo, así como verificar periódicamente dicho sistema o medidas implantadas (art. 24.1. o 32.1.d RGPD).

En nuestro contexto, donde además cada vez resulta mayor la dependencia prestadores de servicios terceros, especialmente en el ámbito de las nuevas tecnologías -muchas de ellas en vanguardia- el entorno legislativo es cada vez más profuso y el impacto de incumplimiento de regulación más intenso que nunca, **se hace necesario elaborar nuestro propio "programa de cumplimiento"** no solo para garantizar el cumplimiento de las obligaciones legales, sino para mejorar nuestras medidas internas de control, obtener una mayor reputación en el sector, evitar el fraude interno así como también posibles sanciones administrativas y/o judiciales.

A los anteriores efectos, el deber de diligencia de la Universidad debe extremarse y, de ahí, la necesidad de dotarnos de políticas de externalización de servicios y evaluación de proveedores que nos ayuden a analizar y evaluar los riesgos, controlar y supervisar a los proveedores que accedan a datos personales a lo largo de todo el ciclo de vida de la propia prestación de servicios que realicen (elección del proveedor, negociación y firma de contrato, monitorización y vigilancia del cumplimiento del contrato, terminación de la prestación de servicios, etc.) e incluso a determinar conjuntamente con los proveedores los controles de los riesgos.

La protección de datos se convierte así, en otro **elemento fundamental previo a la selección nuestros proveedores**, junto con las ya tradicionales cuestiones financieras o logísticas.

El objeto del presente documento es, por tanto, establecer unas **pautas generales, recomendaciones o buenas prácticas** que permitan a los distintas Unidades o Servicios de

la Universidad de Huelva concretar e implementar ese principio general de la diligencia debida a la hora de seleccionar prestadores terceros que hayan de tener acceso a información de carácter personal responsabilidad de la UHU.

El cumplimiento

¿QUÉ SE DEBE VALORAR?

A diferencia del régimen normativo anterior, basado exclusivamente en un cumplimiento meramente formal y/o contractual, el RGPD da un paso más en su **enfoque de riesgos** y exige una mayor responsabilidad y control a los responsables y encargados no solamente al momento contractual sino también a los momentos anteriores y posteriores a la firma del contrato, e incluso en el momento de la terminación de dicha relación o prestación de servicios.

Por eso, la Universidad de Huelva, de acuerdo con lo previsto en el art. 28 RGPD, va a ser responsable de que su proveedor/encargado del tratamiento (en los tratamientos que por cuenta nuestra realice) cumpla con el RGPD. En este sentido, las Directrices para la elaboración de contratos entre responsables y encargados de tratamiento elaboradas por la AEPD, APDCAT y AVPD señalan que **el RGPD establece una obligación de diligencia debida en la elección de los encargados de tratamiento que deben aplicar todos los responsables, contratando únicamente encargados que estén en condiciones cumplir con el RGPD**. Y ello, implica la necesidad de valorar si los encargados con los que se hayan contratado o se vayan a contratar operaciones de tratamiento ofrecen garantías de cumplimiento del RGPD.

La Universidad de Huelva, responsable del tratamiento, debe valorar, controlar y supervisar que su proveedor está utilizando y accediendo a datos personales, en los términos exigidos por el RGPD.

Esa valoración de cumplimiento de los proveedores, encargados de tratamiento, deberá realizarse **con carácter previo y anticipado a la puesta en marcha del correspondiente tratamiento o prestación de servicios** por parte del proveedor y deberá comprender, entre otros, los siguientes análisis o tareas:

- Que en el uso de la información personal se respetan los principios establecidos en el Reglamento General de Protección de Datos (artículo 5 RGPD) **«Principios relativos al tratamiento»**
- Que se han previsto y adoptado un conjunto de Medidas de seguridad, técnicas y organizativas (artículo 32 RGPD) **«Seguridad del tratamiento»**
- Que dichas medidas de seguridad se van a verificar y revisar periódicamente (artículo 24.1 RGPD) **«Responsabilidad del responsable del tratamiento»**

- Que existen determinadas Políticas internas y procedimiento que permitan cumplir con la privacidad desde el diseño (artículo 25 RGPD) **«Protección de datos desde el diseño y por defecto»**

- Que cuenta con un Registro de Actividades de tratamiento, en los casos que resulte necesario (artículo 30 RGPD) **«Registro de las actividades de tratamiento»**

- Que cuentan, en los casos exigidos, con un Delegado de Protección de Datos (Sección 4 | artículos 37-39 RGPD) **«Delegado de protección de datos»**

- Que se van a notificar y/o comunicar las de Brechas de seguridad que, en su caso, pudieran producirse (artículos 33 y 34 RGPD) **«Notificación a la Autoridad de Control y comunicación al interesado de una violación de seguridad de los datos personales»**

- Que se han llevado a cabo los pertinentes análisis de riesgos y/o evaluaciones de impacto (artículo 35 RGPD) **«Evaluación de impacto relativa a la protección de datos»**

- Que se realizan o no Transferencias internacionales de datos (artículo 44 RGPD) **«Principio general de las transferencias»**

PRUEBAS DEL CUMPLIMIENTO

Ahora bien, esa actuación diligente a la hora de elegir proveedor/encargado de tratamiento no puede quedar solamente en la valoración del cumplimiento expuesta en el anterior apartado, sino que además el responsable del tratamiento, y por extensión el propio encargado o subencargado, deben demostrar y acreditar que efectivamente cumplen con la normativa aplicable.

Es decir, no basta únicamente con firmar un contrato en las que se especifique que se cumple con lo establecido en el artículo 28 de RGPD, sino que, para cumplir con el principio de responsabilidad proactiva, es necesario demostrar que los intervinientes tienen implementada una fuerte “cultura de cumplimiento” y que tienen establecidos procedimientos de control y supervisión capaces de probar su eficacia.

En este sentido, a fin de poder demostrar cumplimiento, **el propio RGPD nos da algunas pautas o indicaciones**, de lo que en determinados ámbitos resulta obligatorio tanto para responsables como para encargados, a saber:

- Adopción e **implantación de determinadas medidas** como: seudonimización, minimización/reducción de tratamientos, transparencia, supervisión de tratamientos, promoción de desarrollo y fabricación de productos con una privacidad por defecto, etc. (considerando 78 RGPD).

- Revisión y **actualización de medidas o controles** que garanticen la seguridad del tratamiento (considerando 81 y artículo 24.1 RGPD), previamente determinados y/o exigido al prestador del servicio.

- Contar con un **Registro de actividades de tratamiento** (considerando 82)

- Adoptar las **garantías adecuadas** en los casos de estar ante una transferencia internacional de datos (decisión de la comisión, cláusulas contractuales tipo, etc. (considerando 108)

Metodología de evaluación

Es necesario tener en cuenta que no hay un listado *numerus clausus*, por lo que la comprobación del cumplimiento de la normativa del encargado podrá llevarse a cabo de diferentes modos. Se podrá adaptar dicha evaluación, reforzando el componente técnico, cuando por ejemplo los tratamientos impliquen importantes medidas de seguridad (proveedores de ingeniería, servicios de Cloud), o poner el foco en la relación con usuarios finales, clausulas informativas, comunicaciones oficiales en los casos en los que el tratamiento está relacionado, por ejemplo, con la gestión de datos de nuestros alumnos. No obstante, no hay que olvidar que no todos los proveedores tendrán el mismo carácter de obligatoriedad para el cumplimiento de la normativa.

A continuación, se propone un posible esquema a seguir en la evaluación de proveedores:

ORGANIZACIÓN Y GOBERNANZA DE LA PRIVACIDAD

El proceso ha de incluir la evaluación de la organización y gobernanza de la privacidad del proveedor, verificando y revisando la existencia de criterios relativos a protección de datos y otros aspectos del gobierno y cumplimiento de la normativa como, por ejemplo:

- La posible **adhesión a códigos de conducta**.
- La posesión de un **certificado de protección de datos**.
- En su caso, el **nombramiento de DPD** y su registro ante la autoridad de control competente.
- La realización o no de **Transferencias Internacionales de Datos**, y en tal caso la existencia de **garantías adecuadas** para llevarla a cabo de acuerdo con la regulación.
- La llevanza de un **Registro de Actividades de Tratamiento**.
- La implementación de **políticas internas** relativas al tratamiento de datos personales (ejercicios de derechos, comunicación de incidentes de seguridad, gestión de personal etc.).
- La existencia de **posibles subcontrataciones** (subencargados del tratamiento y los correspondientes acuerdos de protección de datos con terceros).
- La existencia de **antiguas sanciones** al encargado del tratamiento en materia de protección de datos.
- La existencia de **sentencias condenatorias y/o procedimientos judiciales abiertos** en materia de protección de datos respecto del encargado del tratamiento.

Cada uno de los requisitos examinados deberá ir acompañado de los preceptivos comentarios por parte de la persona responsable en el proveedor, así como de la evidencia que justifique dicho cumplimiento.

GESTIÓN DE NEGOCIO

A continuación, se ha de evaluar (en mayor o menor medida) la gestión diaria de la privacidad por parte del proveedor, es decir se examinarán las medidas de seguridad implementadas y el cumplimiento de los requisitos del RGPD, como por ejemplo los mecanismos para el ejercicio de derechos.

En el artículo 28 (“Encargado del tratamiento”) del RGPD, se especifica que el tercero ha de «tomar las medidas necesarias de conformidad con el artículo 32» (el artículo del Reglamento referente a la obligación de implementar las medidas técnicas y organizativas durante el tratamiento), por lo que es necesario implementar en las evaluaciones a terceros (y dejar evidencia) como mínimo las revisiones referentes a:

- **Pseudonimizacion y cifrado de datos personales**: En que ocasiones se utiliza cifrado de datos y/o pseudonimizacion por parte del proveedor de los datos personales (por ejemplo, en los entornos de pruebas, o cuando se trata de categorías especiales de datos).
- **Capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanente de los sistemas y servicios de tratamiento**: Qué medidas técnicas tiene implementadas el proveedor (por ejemplo, controles de seguridad, copias de seguridad periódicas, elementos en alta disponibilidad, sistemas de anti-malware, etc.)
- **Capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico**: La existencia o no de Planes de continuidad de negocio o desastre o procedimientos/políticas de copias de seguridad.

RESPUESTA A INCIDENTES

Otro de los puntos más importantes a la hora de evaluar a los proveedores es la gestión de incidentes de privacidad (cómo actuarían en caso de pérdida de datos o robo de información, por ejemplo). Será necesario evaluar si el proveedor cuenta con procedimientos al respecto y si están implementados correctamente los canales que permitan al responsable cumplir con los requisitos del RGPD, tanto en forma como en tiempo, en caso de que el incidente se produzca en el lado del proveedor.

SEGURIDAD IT

Tal y como señalábamos, los proveedores, deben ofrecer garantías suficientes para aplicar medidas técnicas de manera que el tratamiento sea conforme a lo que exige el reglamento.

Estas medidas deberán ser revisadas y cuyo alcance podrá incluir, entre otros, algunos de los controles que a continuación y a modo de ejemplo se enumeran:

- La existencia de un **control de acceso a los entornos** tanto a nivel físico como lógico mediante identificador único de usuario.
- Limitación los accesos por **roles de funciones**.
- **Registro de accesos** mediante logs (trazables).
- Conservación de **datos pseudonimizados**.
- Backups cifrados en entornos separados, y comunicaciones, utilizando **redes VPNs** basadas en IPSEC o SSL.

Las medidas también podrán ser validadas mediante garantías tales como certificados ISO/IEC como la norma 27001, para acreditar la seguridad en los sistemas de información, y más específicamente con la norma 27701 que contiene requerimientos adicionales de privacidad.

GESTIÓN DEL PERSONAL

Se deberá comprobar que el personal del tercero que participe en el tratamiento de los datos además de las obligaciones identificadas por el responsable cumpla con las obligaciones establecidas por el proveedor que estarán reflejadas en la política de seguridad y procedimientos específicos del mismo.

Algunas de estas obligaciones podrían ser los planes que deben seguir sus empleados ante incidentes de seguridad, **mantener el compromiso de actuar con confidencialidad y no divulgación de información sensible de terceros**, además de incorporar buenas prácticas como: ser cuidadoso con las credenciales de acceso, uso adecuado del correo electrónico y dispositivos externos o destrucción de documentación de forma segura.

SUBCONTRATACIÓN

Una exigencia del RGPD es la autorización previa y por escrito del responsable del tratamiento para que el proveedor pueda recurrir a otro encargado del tratamiento o subencargado. Previo a la fase contractual, se podrá establecer como criterio para la contratación con el responsable que los subencargados estén sujetos a las mismas condiciones que se apliquen al encargado entre ellas las medias de seguridad y obligaciones, anteriormente señaladas, las cuales se harán extensivas a toda la cadena de subcontrataciones que pudiera estar involucrada en el tratamiento.

En cualquier caso, las entidades que vayan a contratar con un proveedor que tras pasar el procedimiento de homologación no cumpla con los requisitos establecidos en el mismo,

En ningún caso, las necesidades o conveniencias de la Universidad puedan obviar o restarle importancia a esta obligación de diligencia respecto a la protección de los datos de carácter personal.

Cumplimiento del artículo 28, RGPD

El Encargado del Tratamiento puede realizar todos los tratamientos que la Universidad le haya encomendado formalmente y debe cumplir con las instrucciones de la misma, que es la única que puede variar las finalidades y los usos de dichos datos personales, teniendo que responder de ellos en todo momento.

Esa dirección y control que la Universidad ejerce sobre el Encargado deben de quedar bien delimitadas, de ahí que el RGPD haya optado por exigir a ambos que regulen su relación a través de un contrato de encargo de tratamiento o de un acto jurídico similar que los vincule y, expresamente y como novedad destacada, exige su formalización por escrito, inclusive en formato electrónico.

PARTICULARIDADES DEL CONTRATO DE ENCARGO DE TRATAMIENTO

El artículo 28 RGPD establece que el contrato de encargo de tratamiento debe contener como mínimo:

- Una descripción suficientemente detallada del mandato al encargado del tratamiento: **el objeto, la duración, la naturaleza y finalidad del tratamiento**.
- Una relación de **medidas técnicas y organizativas adoptadas** por el encargado del tratamiento.
- Una descripción suficientemente detallada de los datos personales objeto del tratamiento: **la tipología de datos y categorías de interesados**.
- Las **obligaciones y derechos de las partes**.

Resulta importante evitar el riesgo de utilización de modelos y exigencias que solo quedarán en el papel del contrato, por no realistas o irrealizables. Cláusulas exigentes que no se exigen, contaminan la credibilidad del contrato y la verdadera intención de las partes, que ya no será la de su obligado cumplimiento.

A efectos prácticos, el Titulo III del Reglamento de Protección de Datos de la Universidad de Huelva, regula el procedimiento de comunicaciones y acceso de datos personales responsabilidad de la Universidad por parte de terceros.

Para la formalización se pueden utilizar los modelos dispuestos en el citado Reglamento:

- **ANEXO III. B.** Texto tipo para pliego de cláusulas administrativas particulares
- **ANEXO IV.** Modelo de contrato-tipo de encargado de tratamiento.

En el caso de que la prestación de **servicio no necesite acceso a datos personales**, pero el prestador del servicio pueda **acceder indirectamente a los mismos**, no sería necesaria la firma de un contrato de encargo de tratamiento, sino únicamente de una **Clausula de Prestación de Servicio sin Acceso a Datos**, es decir, de una cláusula de confidencialidad que obligue al proveedor en caso de que accidentalmente tenga acceso a datos personales durante el desarrollo de los servicios prestados.

- **ANEXO III. A.** Texto tipo para contratos administrativos que no impliquen tratamiento de datos personales.

Aspectos Internacionales

Una cuestión muy relevante a la hora de negociar contratos entre Responsables y Encargados del Tratamiento en un mundo globalizado como el actual, es la consideración de los aspectos internacionales que puedan existir.

En nuestro ámbito, la Universidad (Responsable del tratamiento con establecimiento en la Unión Europea), a la que le resulta de aplicación el RGPD, si va a contratar a un proveedor que vaya a tratar datos en su nombre y por su cuenta como Encargado del Tratamiento, y este encargado está ubicado fuera de la Unión Europea, tiene que asegurarse de firmar un contrato con todos los requisitos del art. 28 (3) del RGPD.

Desde un punto de vista práctico, la mayor parte de los prestadores de servicios de fuera de la Unión Europea y con gran impacto en el tratamiento de datos (por ejemplo, proveedores de servicios de computación en nube) que dirigen sus servicios a clientes corporativos (empresas o Administraciones Públicas) de la Unión Europea, ya contemplan en sus modelos de contratos o condiciones generales de contratación un clausulado específico orientado a cumplir con el art. 28 del RGPD.

REGULACIÓN DE LAS TRANSFERENCIAS INTERNACIONALES

Son muchos los casos en los que pueden llegar a darse transferencias internacionales con motivo de la prestación del servicio de un Encargado y que habrán de haber sido objeto detallado de negociación entre las partes, dada su especial trascendencia. Algunas cuestiones relevantes:

- Regular en el contrato la **ubicación de las personas que van a prestar los servicios**, especialmente cuando estos puedan ser prestados en remoto, a través de teletrabajo o similar que permitan la ubicación del personal en un lugar distinto del de el establecimiento principal del proveedor.
- La **ubicación de los datos personales** es un factor clave a la hora de negociar el contrato (especial importancia en cuanto a la ubicación física de los servidores o data centers en contratos de computación en nube o tecnológicos), de cara a: recoger en el mismo que estarán ubicados en los territorios de la Unión Europea o considerados con protección equiparable y que esto sea una de las cuestiones a controlar durante la ejecución del contrato; o bien, regular en el propio contrato la transferencia internacional, habitualmente mediante la inclusión de las cláusulas contractuales tipo en un anexo al contrato o documento independiente a firmar en un mismo acto con el Contrato de Encargo de tratamiento, o si se tratase de una transferencia internacional por un tratamiento de un subencargado, que se incluya la autorización para firmar las

cláusulas contractuales tipo o se incluya una referencia a las normas corporativas vinculantes si se tratase de entidades del mismo grupo empresarial.

De cara a cubrir los riesgos por este tipo de casuísticas, es común solicitar a los Encargados del tratamiento una evidencia de las cláusulas contractuales tipo que ha firmado con sus subcontratistas o una referencia a la publicación de la autoridad que ha aprobado las normas corporativas vinculantes.

Controles periódicos

Buscar mejoras en el proceso de desempeño específico de los encargados de tratamiento, ayudará a la Universidad de Huelva, como Responsable del Tratamiento, a crear relaciones duraderas y desarrollar las competencias de ambas partes en un ambiente de confianza y cumplimiento. Seguimiento y Control, estos dos conceptos son una excelente combinación para poder disminuir o evitar problemas con nuestros proveedores, que deberán constar expresa y detalladamente en cada Contrato de Encargo de tratamiento para hacerlos exigibles a las partes.

Toma de decisiones sobrevenidas ante situaciones imprevistas

Tanto en el momento de fijar las estipulaciones del Contrato de Encargo de tratamiento como durante toda la vida del mismo, la Universidad, como Responsable, y el proveedor Encargado deberán tener en cuenta que sus actos podrán ser considerados un cumplimiento o incumplimiento de las normas que lo rigen: (i) normas administrativas que rigen el contenido y cumplimiento de estos, RGPD y LOPDGDD; y (ii) el principio de autonomía de la voluntad en los contratos del artículo 1.255 del Código Civil.

Las cláusulas que rijan las obligaciones entre Responsable y Encargado en los Contratos de Encargo de Tratamiento, siempre estarán condicionadas por la normativa sobre protección de datos personales y el régimen sancionador por su incumplimiento, en función de su gravedad, de conformidad con lo establecido en la LOPDGDD:

Son **infracciones graves**:

- Contratar a un encargado que no ofrezca garantías suficientes (art 73 j).
- Encargar el tratamiento a un tercero sin haber formalizado antes un contrato o un acto jurídico por escrito (art. 73 k).
- Que un encargado contrate a otros sin contar con la autorización o información previa del responsable (art. 73 l).
- La infracción al determinar los fines y medios del tratamiento (art. 73 m) cambiando la consideración del encargado a responsable (RGPD art. 28.10).

Son **infracciones leves**:

- No informar al responsable sobre la posible infracción de la normativa sobre protección por una instrucción recibida de este (art. 74 j).

— El incumplimiento de las estipulaciones del contrato u otro acto jurídico que regula el tratamiento o las instrucciones dadas por el responsable, salvo que esté obligado por la normativa y lo hubiera advertido al responsable o al encargado del tratamiento (art. 74 k).

En consecuencia, el Contrato de Encargo de tratamiento deberá establecer directrices de cómo actuar entre el Responsable y los Encargados antes las situaciones imprevistas:

- Consultas a las Autoridades de Control.
- Apertura de expediente o sanción por parte de las Autoridades de Control.
- Brechas de seguridad.
- Modificaciones significativas en la prestación del servicio.
- Extinciones o fusiones, cambios de denominación social, cesiones, etc.
- Oposición a las auditorías u otros controles o resultados de esas auditorías/controles que resulten en la detección de un riesgo para el tratamiento de los datos personales objeto del contrato.
- Potencial arbitraje tecnológico.

Conclusiones

Según se exponía en la introducción, se ha presentado una propuesta de cómo abordar de manera la práctica la gestión del riesgo de terceros en el ámbito de la privacidad; como también se ha indicado, se ciñe el concepto de “tercero” al de “encargado del tratamiento”, definido en el artículo 4.8 RGPD como “la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento”.

Las funciones que desarrollan nuestros encargados serán realizadas por cuenta de la Universidad, que es la responsable, de forma que será ésta y no el encargado el que tome las decisiones en relación con los elementos esenciales del tratamiento (fines y medios del tratamiento).

El artículo 28 del RGPD obliga al responsable a elegir únicamente a aquellos encargados que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de tal manera que el tratamiento que realicen por cuenta del responsable sea conforme con los requisitos establecidos en la citada normativa.

Precepto que encuentra su justificación en el art. 5.2. RGPD que recoge el principio básico de la “responsabilidad proactiva” o *accountability*, tradicionalmente conocido también como “obligación de diligencia debida”.

En consecuencia, el RGPD da un paso más en su enfoque de riesgos y exige una mayor responsabilidad y control a los responsables y encargados; no solamente en el momento meramente contractual sino también a en los momentos anteriores y posteriores a la firma del contrato, e incluso en el momento de la terminación de dicha relación o prestación de servicios.

Por esta razón, antes de compartir datos de carácter personal con terceros, la Universidad de Huelva (responsable del tratamiento) debe llevar a cabo una evaluación de riesgo de los mismos, en la que debe quedar todo perfectamente documentado a fin de poder acreditar en todo momento tanto la debida diligencia como las decisiones y actuaciones llevadas a cabo.

ANEXO

CUESTIONARIO PARA LA EVALUACIÓN DE PRESTADORES DE SERVICIOS CON ACCESO A DATOS DE CARÁCTER PERSONAL

En cumplimento del principio de responsabilidad activa y diligencia en la elección de proveedores con acceso a datos de carácter personal (encargados del tratamiento) establecido en 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 – Reglamento General de Protección de Datos (RGPD), la Universidad de Huelva precisa conocer su grado de adaptación a esta normativa. Así mismo, la Universidad de Huelva se reserva el derecho de poder solicitar información complementaria para acreditar el cumplimiento de las exigencias establecidas en el RGPD.

Identificación del prestador de servicios

Denominación de la entidad:	
Domicilio social:	CIF/NIF:

Datos de contacto (Interlocutor y/Delegado de Protección de Datos)

Nombre, apellidos, número de teléfono y dirección de correo electrónico de la persona designada por el prestador de servicios para la resolución de las consultas y/o cuestiones en materia de protección de datos y/o del Delegado de Protección de Datos (indicar si la persona de contacto ha sido designada formalmente como DPD o no). En caso de ser dos personas diferentes, indicar los datos de ambos.		
1	Nombre y apellidos:	
Correo electrónico:		Teléfono:
2	Nombre y apellidos:	
Correo electrónico:		Teléfono:

Información sobre el tratamiento de datos en la prestación del servicio

SERVICIOS A PRESTAR
Servicios que prestará como Encargado a la Universidad de Huelva (breve descripción)

Si alguna de las preguntas realizadas en el cuestionario no es de aplicación según los servicios prestados por su entidad especifique: "No aplica".

CATEGORÍAS DE DATOS PERSONALES A LOS QUE TENDRÁ ACCESO					
Datos personales de carácter identificativo					
☐	Nombre y apellidos	☐	Dirección electrónica	☐	Tarjeta sanitaria
☐	DNI/Pasaporte o similar	☐	Firma	☐	Marcas físicas
☐	Teléfono	☐	Firma electrónica	☐	Imagen/voz
☐	Dirección	☐	Nº SS / mutualidad	☐	Huella digital
☐	Otros *(especificar)*				
Datos de categorías especiales					
☐	Origen étnico o racial	☐	Afiliación sindical	☐	Datos relativos a la salud
☐	Ideología u opiniones políticas	☐	Datos genéticos	☐	Datos relativos a la vida sexual
☐	Convicciones religiosas o filosóficas	☐	Datos biométricos (identificación unívoca)	☐	Datos sobre orientación sexual
Otros datos personales					
☐	Académicos y profesionales	☐	Características personales	☐	Circunstancias sociales
☐	Económicos, financieros y de seguros	☐	Información de análisis	☐	Información comercial
☐	Transacciones de bienes y servicios	☐	Información de scoring o perfilado	☐	Detalles del empleo
☐	Otros *(especificar)*				

LOCALIZACIÓN Y UBICACIÓN DE LOS TRATAMIENTOS DE DATOS
Indique la totalidad de las ubicaciones en las que realizará tratamiento (incluyendo almacenamiento y conservación) de datos para la prestación de servicios a la Universidad de Huelva.

SUBCONTRATISTAS DEL ENCARGADO DEL TRATAMIENTO
Indique todos los subcontratistas (incluyendo prestadores de servicios, otras empresas del grupo, etc…) que intervendrán en la prestación del servicio a la Universidad de Huelva.

Adecuación al RGPD del Prestador

RESPONSABILIDAD PROACTIVA
Detallar las acciones llevadas a cabo por el prestador de servicios para el cumplimiento del principio de Responsabilidad Proactiva del RGPD.

POLÍTICAS Y PROCEDIMIENTOS
Describa brevemente las políticas aplicadas y planes de actuación para dar cumplimiento al RGPD. En el supuesto de que las mismas no estén implantadas, indique el plazo o fecha en que serán efectivas y el medio por el cual se comunicarán a la Universidad de Huelva.

CÓDIGOS DE CONDUCTA Y CERTIFICADOS DE PRIVACIDAD
Especifique los códigos de conducta o certificados de privacidad o seguridad (Certificación ENS, ISO 27001, ISO 22001, etc.) con los que cuenta su entidad, se encuentra adherido o en proceso de obtención.

Relaciones con la Universidad de Huelva

SISTEMAS/ APLICATIVOS A UTILIZAR
Indicar los sistemas y/o aplicativos utilizados para la prestación del servicio a la Universidad de Huelva.

COLABORACIÓN CON LA UNIVERSIDAD DE HUELVA
Indicar los procedimientos o medidas que aplica o prevé aplicar con el fin de garantizar que en la prestación de los servicios la Universidad de Huelva cumple con el RGPD. Concretamente, exponga los procesos o medidas concernientes a: — *Principio de privacidad por diseño y por defecto.* — *Procedimientos para el efectivo ejercicio de los derechos de las personas afectadas.* — *Transparencia del tratamiento (deber de informar).*

NOTIFICACIÓN DE BRECHAS DE SEGURIDAD (VIOLACIONES DE SEGURIDAD)
Indicar los procedimientos de notificación de brechas de seguridad en la entidad de acuerdo con lo previsto en el RGPD, incluyendo, entre ellos, la comunicación a la Universidad de Huelva.

Medidas de Seguridad

Indique si se han implementado las siguientes medidas de seguridad en los sistemas:

☐ CONTROL DE ACCESOS FÍSICO AL CPD

Describir

☐ MEDIDAS DE PROTECCIÓN FÍSICA EN CPD

Describir las medidas

☐ GESTIÓN DE SOPORTES

Inventario actualizado de soportes, *cifrado de soportes, borrado seguro de soportes,…*

☐ CONTROL DE ACCESOS LÓGICOS A SISTEMA OPERATIVO Y APLICACIONES

Administradores y usuarios, segregación de funciones, Políticas de contraseñas,…

☐ REGISTROS DE ACCESOS A APLICACIONES Y BASES DE DATOS

Comentarios

☐ COPIA DE SEGURIDAD

Frecuencia y ubicación de las copias

☐ PROCEDIMIENTO DE CONTINUIDAD DE NEGOCIO

Comentarios

☐ GESTIÓN DE INCIDENCIAS

Registro y notificación de brechas de seguridad

☐ COMUNICACIONES CIFRADAS

Comentarios

☐ AUDITORÍA TÉCNICA DE SISTEMAS Y PENTESTING

Comentarios

☐ GESTIÓN DE VULNERABILIDADES DE SISTEMAS Y APLICACIONES

Comentarios

☐ CIFRADO EN EQUIPOS Y DISPOSITIVOS MÓVILES

Comentarios

☐ SEGURIDAD EN ENTORNOS DE DESARROLLO Y TEST

Comentarios

☐ PSEUDOANONIMIZACIÓN / ANONIMIZACIÓN DE DATOS PERSONALES

Comentarios

☐ GESTIÓN DE INCIDENCIAS

Comentarios

☐ OTRAS MEDIDAS DE SEGURIDAD

Describir

Observaciones

Observaciones o comentarios:

Fecha y firma del Prestador.

Documentos adjuntos
