

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN DE LA SECRETARÍA TÉCNICA SOBRE LA GESTIÓN DE INFORMACIÓN, ANÁLISIS DE RIESGOS Y RIESGOS ASOCIADOS PARA LA FUNDACIÓN HAZI.

1. OBJETO DEL CONTRATO

El presente pliego recoge el detalle de los requisitos técnicos MINIMOS que debe cumplir el servicio ofertado, las condiciones suministro y de garantía del mismo. Estos requisitos van detallados en el Anexo I:

2. ANEXO I

- Delegado de protección de datos de carácter personal.
 - Esta figura, conocida como DPO (acrónimo inglés de Data Protection Officer), constituye uno de los elementos claves del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 de Protección de Datos (en lo sucesivo, RGPD), y un garante del cumplimiento de la normativa de la protección de datos en las organizaciones, sin sustituir las funciones que desarrollan las Autoridades de Control. A tal efecto, el servicio de DPD objeto de la presente contratación deberá, de forma independiente, asumir las funciones reguladas en el artículo 39 del RGPD, entre las que destacan informar y asesorar, así como supervisar el cumplimiento del citado RGPD por parte del responsable o encargado del tratamiento de datos de la EC. Por su parte la EC y en concreto los responsables o los encargados de tratamiento, tendrán la obligación de facilitar al DPD todos los recursos necesarios para desarrollo de su actividad.
 - De acuerdo con lo dispuesto en el RGPD, las funciones del DPD se circunscriben a las siguientes tareas generales:
 - Informar y asesorar a los responsables o a los encargados de los tratamientos y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del RGPD y de otras disposiciones de protección de datos de la Unión Europea o de los Estados miembros.
 - Supervisar el cumplimiento de lo dispuesto en el citado Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales.

- Estas funciones generales de DPD se concretan, de manera fundamental, en las siguientes tareas particulares:
 - Cumplimiento de principios relativos al tratamiento, como los de limitación de finalidad, minimización o exactitud de los datos.
 - Identificación de las bases jurídicas de los tratamientos.
 - Valoración de compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos.
 - Detección de la existencia de normativa sectorial que pueda determinar condiciones de tratamiento específicas distintas de las establecidas por la normativa general de protección de datos.
 - Elaboración de un modelo de diseño e implantación de medidas de información a los afectados por los tratamientos de datos.
 - Establecimiento de mecanismos de recepción y gestión de las solicitudes de ejercicio de derechos por parte de los interesados.
 - Valoración de las solicitudes de ejercicio de derechos por parte de los interesados.
 - Asesorar y supervisar la contratación de encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación responsable-encargado.
 - Identificación de los instrumentos de transferencia internacional de datos adecuados a las necesidades y características de la organización y de las razones que justifiquen la transferencia.
 - Auditoría de protección de datos.
 - Establecimiento y gestión de los registros de actividades de tratamiento.
 - Análisis de riesgo de los tratamientos realizados.
 - Asesoramiento en la implantación de las medidas de

protección adecuadas a los riesgos y naturaleza de los tratamientos.

- Establecimiento de procedimientos de gestión de violaciones de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de los afectados y los procedimientos de notificación a las autoridades de supervisión y a los afectados.
- Determinación de la necesidad de realización de evaluaciones de impacto sobre la protección de datos y su realización.
- Relaciones con las autoridades de supervisión.
- Asesoramiento en la implantación de programas de formación y sensibilización del personal en materia de protección de datos.

- La adjudicataria del presente contrato deberá realizar los siguientes trabajos:
 - Actuaciones a realizar por la adjudicataria del servicio en materia de cumplimiento normativo en protección de datos.
 - Revisar el Registro de Actividades de Tratamiento de la organización en su conjunto, verificando y actualizando contenidos existentes e identificando nuevos tratamientos que se hubieran desarrollado por la organización, con especial apreciación de normativa sectorial en el ámbito de las ayudas a los sectores involucrados, y que pueda determinar condiciones de tratamiento específicas integrables en la normativa general de protección de datos.
 - Verificar la definición de procedimientos específicos que, partiendo de los existentes se adapten a las nuevas exigencias prácticas del RGPD y sean compatibles, y por tanto integrables, con los desarrollados en el marco del ENS, constituyendo un conjunto procedimental único asociado a la seguridad y privacidad.
 - Realizar los análisis de riesgo y de evaluaciones de impacto sobre la privacidad que garantice que todos los tratamientos consideren dicho impacto de manera asociada a la valoración de los servicios llevada a cabo desde el punto de vista del ENS, con el fin de que ambos aspectos queden completamente integrados.
 - Reforzar los mecanismos que garanticen la aplicación de los principios de privacidad desde el diseño en los productos, servicios y recursos de

la organización, como medida de responsabilidad proactiva basada en la anticipación que exige el RGPD.

- Actualizar el protocolo de conducta o adecuado tratamiento de datos personales referido al personal directivo y empleado de la organización.
 - Verificar los aspectos vinculados al teletrabajo, videollamadas u otros sistemas fuera de las dependencias o sedes corporativas.
 - Elaboración de cuantas medidas correctoras técnicas u organizativas, actuaciones y protocolos se deriven de los resultados de los análisis de riesgos y evaluaciones de impacto sobre la privacidad.
- Actuaciones a realizar por la adjudicataria del servicio en materia de publicidad y gestión de las “cookies”.
- El año 2020 ha constituido un momento esencial respecto a la utilización de herramientas de publicidad digital, dado que se ha implantado por la Agencia Española de Protección de Datos un nuevo sistema de aviso y contenido informativo del uso de cookies, debiendo las organizaciones actualizar sus sistemas y contenidos de información basados en cookies, definiendo procesos más respetuosos y precisos vinculados al consentimiento expreso de la persona y a su gestión.
 - Además, la utilización de información derivada del uso de cookies por parte de las organizaciones constituye un desafío importante al evidenciarse el conflicto entre analizar cada vez mayor volumen de información personal, y a ser posible personalizada, y respetar las exigencias de adecuada información y gestión imponen límites a este uso indiscriminado.
 - HAZI tiene desplegados y despliega distintos sistemas de información accesibles por personas usuarias que debe ser analizado a fin de revisar su adecuación a la normativa y políticas de protección adoptadas por la EC.
- Asistencia en la interpretación de las previsiones que realiza la LOPDGDD sobre los derechos digitales, y en particular sobre cualquier iniciativa de monitorización, grabación de actividades o control laboral que quiera implantar la organización.
- La Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales establece una serie de elementos innovadores en el

ordenamiento jurídico, en un formato de nuevos derechos relacionados con la existencia de las plataformas digitales. Estos derechos afectan a diversos colectivos (personal empleado, personas con las que se relaciona la Fundación) y es preciso tenerlo en cuenta.

- Por otra parte, la jurisprudencia ha modificado muchos de sus parámetros y se pide que la empresa adjudicataria conozca el sector y pueda informar a la Fundación de las condiciones de aplicación de estos nuevos derechos.
- Asistencia en la gestión de datos en materia de líneas de ayudas, y en la preparación de auditorías realizadas por organismos autonómicos, nacionales o internacionales, en el marco de los distintos proyectos o gestión de ayudas que realice la fundación, y en concreto del Organismo Pagador de Euskadi.
 - La Fundación HAZI participa como ente gestor o distribuidor en distintos proyectos vinculados a la convocatoria o gestión de ayudas económicas para la promoción de los sectores agrícola, ganadero o alimentario.
 - En el marco de estas convocatorias, la Fundación realiza actividades de Secretaria Técnica con mayor o menor incidencia en la operativa ordinaria de la gestión, realizando actuaciones estrictamente de apoyo informático (alojamiento o asistencia tecnológica, como desarrollo de aplicaciones o páginas web) pero también con contenido operativo lo que conlleva normalmente una gran implicación en datos personales, y en su gestión, gestión que por otra parte está controlada y dirigida por el Departamento competente.
- Asistencia a HAZI como encargado de tratamientos del Departamento competente en materia de agricultura, ganadería, pesca y alimentación y/o nuevos tratamientos vinculados con este encargo.
 - La empresa adjudicataria realizará la asistencia jurídica a demanda en cuestiones relacionadas con la protección de datos personales en el marco de la actividad desarrollada por HAZI como Encargado de Tratamiento de este Departamento, realizando informes y resolviendo cuantas dudas se sometan.
 - Las funciones anteriormente descritas se concretan en la siguientes:
 - Cumplimiento de principios relativos al tratamiento, como los de limitación de finalidad, minimización o exactitud de los datos.
 - Identificación de las bases jurídicas de los tratamientos.

- Valoración de compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos.
- Detección de la existencia de normativa sectorial que pueda determinar condiciones del tratamiento específicas distintas de las establecidas por la normativa general de protección de datos.
- Asesorar y supervisar la contratación de encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación responsable-encargado.
- Identificación de los instrumentos de transferencia internacional de datos adecuados a las necesidades y características de la organización y de las razones que justifiquen la transferencia.
- Establecimiento y gestión de los registros de actividades de tratamiento.
- Análisis de riesgo de los tratamientos realizados.
- Asesoramiento en la implantación de las medidas de protección adecuadas a los riesgos y naturaleza de los tratamientos.
- Establecimiento de procedimientos de gestión de violaciones de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de los afectados y los procedimientos de notificación a las autoridades de supervisión y a los afectados.
- Determinación de la necesidad de realización de evaluaciones de impacto sobre la protección de datos y su realización.
- Relaciones con las autoridades de supervisión.
- Asesoramiento en la implantación de programas de formación y sensibilización del personal en materia de protección de datos.