

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA EL ACUERDO MARCO DE ASESORAMIENTO JURÍDICO Y DE MEDIDAS TÉCNICAS Y ORGANIZATIVAS EN MATERIA DE PROTECCIÓN DE DATOS

1. OBJETO DEL ACUERDO MARCO.

El objeto del contrato es la prestación del servicio asistencia jurídica, organizativa, técnica y consultoría para la adecuación de la Diputación Foral de Bizkaia (en adelante BFA-DFB) y sus Entidades Forales a la legislación y procedimientos en materia de protección de los datos personales contemplados 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 y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), así como a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Al mismo tiempo el objeto del presente contrato también consiste en la adecuación de las Entidades Locales del Territorio Histórico de Bizkaia a la normativa anteriormente citada, así como el asesoramiento para la adecuación de la figura del Delegado/a de Protección de datos (en adelante DPO) y los servicios que se definen en la legislación citada para las Entidades Locales adheridas a la Central de Contratación de la Diputación Foral de Bizkaia.

2. NORMATIVA DE APLICACIÓN.

Principal normativa aplicable para la ejecución del proyecto:

- 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). (en adelante RGPD).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. (en adelante LOPD-GDD).
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Real Decreto 3/2010, de 8 de enero (BOE de 29 de enero), por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

3. SERVICIOS A REALIZAR.

Los servicios a realizar se estructuran en 5 lotes con diferentes niveles de servicios.

Las empresas podrán presentar oferta a la totalidad o a algunos de los lotes, pero se adjudicará un máximo de 2 lotes a una misma empresa, por lo que las empresas deberán indicar en su proposición económica el orden de preferencia de los lotes que oferten.



Será excepción a esta regla cuando a consecuencia de su aplicación resultara un lote desierto. En este caso, se adjudicará el lote a la empresa con mayor puntuación aunque fuera adjudicataria de otros dos lotes preferentes.

Se deberá realizar una descripción metodológica completa de la propuesta en una memoria, en la que se describa el alcance y los métodos de trabajo propuestos (30 hojas máx.).

- 3.1 LOTE 1: SERVICIO DE ASISTENCIA JURÍDICA, ORGANIZATIVA, TÉCNICA Y CONSULTORÍA PARA LA ADECUACIÓN DE LA BFA-DFB Y SUS ENTIDADES FORALES A LA LEGISLACIÓN Y PROCEDIMIENTOS EN MATERIA DE PROTECCIÓN DE LOS DATOS PERSONALES.
- 3.2 LOTE 2: SERVICIO DE DPO PARA LAS ENTIDADES LOCALES DEL TERRITORIO HISTÓRICO DE BIZKAIA (GRUPO 1).
- 3.3 LOTE 3: SERVICIO DE DPO PARA LAS ENTIDADES LOCALES DEL TERRITORIO HISTÓRICO DE BIZKAIA (GRUPO 2).
- 3.4 LOTE 4: SERVICIOS ORIENTADOS A LA ADECUACIÓN DE LAS ENTIDADES LOCALES DEL TERRITORIO HISTÓRICO DE BIZKAIA AL RGPD Y A LA LOPD-GDD (GRUPO 3).
- 3.5 LOTE 5 SERVICIOS ORIENTADOS A LA ADECUACIÓN DE LAS ENTIDADES LOCALES DEL TERRITORIO HISTÓRICO DE BIZKAIA AL RGPD Y A LA LOPD-GDD (GRUPO 4).

3.1 LOTE 1: SERVICIO DE ASISTENCIA JURÍDICA, ORGANIZATIVA, TÉCNICA Y CONSULTORÍA PARA LA ADECUACIÓN DE LA BFA-DFB Y SUS ENTIDADES FORALES A LA LEGISLACIÓN Y PROCEDIMIENTOS EN MATERIA DE PROTECCIÓN DE LOS DATOS PERSONALES.

Servicios orientados a la adecuación de la BFA-DFB y sus Entidades Forales al Reglamento General de Protección de Datos, y a la Ley 3/2018 de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Durante el ciclo de vida del contrato la empresa adjudicataria proporcionará asesoramiento jurídico, técnico y organizativo a la Sección de Asesoramiento Jurídico, Seguridad de la Información y Protección de Datos para la efectiva adecuación de los Departamentos de la BFA-DFB así como a las Entidades Forales que, como responsables y encargados de tratamientos de datos personales en el desarrollo de muchas de sus actividades, han de dar cumplimiento a las garantías jurídicas vigentes y a las nuevas incorporadas en el nuevo RGPD y la Ley Orgánica 3/2018. El servicio cubrirá los siguientes ámbitos:



3.1.1 Asesoramiento jurídico-técnico a la sección de Asesoramiento Jurídico, Seguridad de la Información y Protección de Datos. Apoyo presencial, telefónico y telemático a demanda. En concreto:

- ✓ Resolución de dudas y consultas de índole jurídica, organizativa o técnica relacionadas con la materia de protección de datos.
- ✓ Revisión, actualización y propuesta de elaboración de cláusulas o avisos legales, así como de otros documentos o informes relacionados.
- ✓ Elaboración y redacción de la documentación necesaria en materia de política de privacidad.
- ✓ Revisión, actualización y propuesta de elaboración de contratos de acceso a datos (así como otras prestaciones de servicios sin acceso a datos pero que se vean afectadas por lo dispuesto en el RGPD y la Ley Orgánica 3/2018).
- ✓ Asesoramiento, resolución de dudas y consultas de índole jurídica ante posibles cesiones de datos y peticiones de datos a terceras organizaciones o entre los diferentes departamentos de BFA-DFB y sus entidades forales. Redacción de los informes y escritos necesarios.
- ✓ Estudios de aplicación de la normativa de protección de datos en relación con otras normativas, frente a diversas situaciones que pudieran plantearse durante el desarrollo de los proyectos de la organización.
- ✓ Estudio y diseño y redacción de posibles soluciones jurídicas a las cuestiones que en materia de protección de datos, interoperabilidad o legislación asociada a las nuevas tecnologías, se presenten durante el despliegue de los proyectos de la entidad.
- ✓ Asesoramiento, resolución de dudas y consultas de índole jurídica en materias estrechamente relacionadas con la protección de datos, como el derecho a la intimidad, honor e imagen, y los delitos relacionados con las tecnologías.
- ✓ Asesoramiento y colaboración en la elaboración y actualización de las diferentes Normativas de seguridad en materia organizativa, técnica y operativa que afecten a la protección de datos, así como sus anexos, autorizaciones, delegaciones, nombramientos, etc.
- ✓ Colaboración con la persona DPO para las altas, modificaciones y supresiones de tratamientos, previa encuesta y documentación de los mismos.
- ✓ Colaboración con la persona DPO en la coordinación, gestión y control de los procedimientos de Seguridad (incidencias, administración de usuarios, ejercicio de derechos acceso, rectificación, supresión, limitación del tratamiento, portabilidad y oposición.), gestión de soportes, accesos a dependencias, etc.).
- ✓ Realización de informes jurídicos relacionados con la aplicación de la normativa de protección de datos y elaboración de la documentación de posibles transferencias internacionales de datos.
- ✓ Elaboración de una memoria anual en la que se reflejen las actuaciones realizadas.
- ✓ Elaboración de los distintos Planes de Trabajo que sean necesarios para la implementación de las diferentes tareas a abordar.
- ✓ Asesoramiento, y elaboración de propuestas de informes y documentación ante posibles denuncias ante las Autoridades de Control en materia de protección de datos, así como de la documentación que fuese necesaria frente a requerimientos de cualquier tipo solicitados por las Autoridades de Control en materia de protección de datos.



- ✓ Cualquier otra cuestión, que con motivo del desarrollo del proyecto y en relación con la materia de que se trata, sea planteada por los interlocutores autorizados de BFA-DFB.

Para la prestación del servicio, a demanda de BFA-DFB, la empresa adjudicataria garantizará:

- o Asistencia a reuniones internas de seguimiento y de impulso de los trabajos emprendidos. Las reuniones se planificarán en colaboración con la sección. Se deberá garantizar la disponibilidad para acudir a las instalaciones de BFA-DFB en menos de 48 horas para la gestión de situaciones que BFA-DFB determine como urgentes.
- o Preparación y asistencia a reuniones con otros organismos, al objeto de prestar apoyo directo, como asesores jurídicos, a los responsables de BFA-DFB ante dichos organismos.
- o Elaboración de toda la documentación derivada de dichas reuniones, así como el envío de la citada información a BFA-DFB en el formato que determine BFA-DFB

3.1.2 Servicio de consultoría para la adecuación de la BFA-DFB y entidades forales al RGPD y LOPD-GDD.

- ✓ Definición de procedimientos necesarios para la coordinación con los Departamentos de la Diputación Foral. Identificación y gestión de relación con las personas dinamizadoras y responsables de tratamiento, canal de consultas, modelos de solicitud de consulta/tratamientos, gestión documental, definición de informes de reporte tipo, entre otros.
- ✓ Definición de procedimientos necesarios para la coordinación con las entidades forales. Identificación y gestión de relación con responsables de protección de datos y seguridad de la información responsables de tratamiento, canal de consultas, modelos de solicitud de consulta/tratamientos, gestión documental, definición de informes de reporte tipo, entre otros.
- ✓ Revisión, actualización, elaboración e implantación de diferentes tareas que se llevarán a cabo en colaboración con la Sección:
 - a. Revisión, elaboración y actualización del Registro de Actividades de Tratamiento de la BFA-DFB y sus entidades forales así como la realización de propuestas de mejora en relación al citado Registro de Actividades de Tratamiento.
 - b. Identificación y actualización de las finalidades precisas y la base jurídica de los tratamientos que se llevan a cabo en la BFA-DFB y sus entidades forales.
 - c. Identificación de los tratamientos gestionados bajo el principio de consentimiento del interesado y su adecuación a las nuevas exigencias del RGPD y la Ley Orgánica 3/2018.
 - d. Definición, elaboración y actualización para cada proceso: responsables, flujos de información/aprobación, canales, entre otros.
 - e. Elaboración y actualización de plantillas y guías prácticas como apoyo en la implementación de los procesos.
 - f. Revisión elaboración y actualización de las medidas de seguridad que se aplican a los tratamientos, así como elaboración e implementación en colaboración con la Entidad



Foral LANTIK en el diseño de otras medidas de seguridad tanto técnicas como organizativas que eviten la pérdida de información, la destrucción involuntaria de datos o el acceso de un tercero no autorizado, y que a su vez garanticen la integridad, la disponibilidad y la inalterabilidad de los datos tratados.

- g. Procedimentación e implantación así como revisión y actualización del proceso para el ejercicio de derechos de acceso, rectificación, supresión, limitación del tratamiento, portabilidad y oposición, así como de otros que sea necesario identificar e implantar para la correcta aplicación de la normativa de protección de datos.
- h. Revisión, elaboración y actualización de los procedimientos normativos y protocolos necesarios para detectar y gestionar incidencias de seguridad y sus posibles brechas, identificar las que puedan producir fugas de información y las obligaciones al respecto.
- i. Elaboración de cualesquiera otros procedimientos normativos y protocolos de actuación que sean necesarios para el adecuado cumplimiento de la normativa de protección de datos.
- j. Diseño de medidas de seguridad tanto técnicas como organizativas que eviten la pérdida de información, la destrucción involuntaria de datos o el acceso de un tercero no autorizado, y que a su vez garanticen la integridad, la disponibilidad y la inalterabilidad de los datos tratados.
- k. Análisis de riesgos. La Adjudicataria analizará junto con BFA-DFB y sus entidades forales los riesgos en los tratamientos. Como resultado, se obtendrá información relativa a qué riesgos afectan a los tratamientos, de cara a establecer un plan de Tratamiento de Riesgos de mejora o de reducción de riesgos.
- l. La adjudicataria analizará, revisará, y elaborará y actualizará el estudio de los tratamientos para determinar si es necesario realizar la evaluación de impacto en la privacidad.
- m. En el caso que se detecte que alguno de los tratamientos de datos personales genera un alto riesgo para los derechos y libertades de los interesados: la adjudicataria elaborará la documentación necesaria así como los procedimientos necesarios para una evaluación de impacto relativa a la protección de datos para cada uno de ellos.
- n. Plan de mejora. La adjudicataria elaborará un Plan de mejora de Tratamientos de Riesgos para la BFA-DFB y las Entidades Forales. En este Plan, deben priorizarse las medidas orientadas a mitigar riesgos en tratamientos que conlleven un mayor riesgo de lesionar derechos y las libertades de los interesados, en función de la sensibilidad de los datos, del ámbito en que se realiza el tratamiento y del volumen de datos tratados.



3.1.3 Sesiones formativas en materia de protección de datos y también relacionadas con la implantación de los procesos mencionados en el apartado anterior.

- Planificación y organización de sesiones de formación en formato presencial y/u online (a determinar el formato, en cada caso, con la Sección de Asesoramiento Jurídico, Seguridad de la Información y Protección de Datos), dirigidas a los Departamentos forales y entidades forales. Las sesiones de formación dirigidas a los departamentos y entidades forales serán como mínimo 4. La formación deberá proporcionar contenidos teóricos y eminentemente prácticos para la implementación de los procesos definidos para la adecuación al RGPD y LOPD-GDD.
- Elaboración de material didáctico (videos, cartelería, entre otros) y plan de divulgación de los distintos formatos según colectivos (personas dinamizadoras, personal de BFA-DFB, responsables de tratamiento, responsables de protección de datos y seguridad de la información de las entidades forales).

3.1.4 Desarrollo del servicio

Compromiso de tiempo de respuesta a las consultas que se planteen en el marco del asesoramiento jurídico-técnico a la sección de Asesoramiento Jurídico, Seguridad de la Información y Protección de Datos

Se adoptará un compromiso de tiempo de respuesta máxima para las consultas planteadas en función de su complejidad y criticidad. Como mínimo deberán cumplir con los siguientes requisitos:

- El tiempo de resolución variará según la naturaleza de la cuestión formulada:
 - Complejidad baja: 1 hora desde el establecimiento de contacto efectivo.
 - Complejidad media: 1 jornada laboral desde el establecimiento de contacto efectivo.
 - Complejidad alta: 5 jornadas laborales desde el establecimiento de contacto efectivo.
- Para consultas de carácter urgente el criterio anterior será sustituido por el siguiente:
 - Complejidad baja: 1 hora desde el establecimiento de contacto efectivo.
 - Complejidad media: 4 horas desde el establecimiento de contacto efectivo.
 - Complejidad alta: 3 jornadas laborales desde el establecimiento de contacto efectivo.

Entregables

La empresa adjudicataria proporcionará un cronograma orientativo para la prestación del servicio, con indicación, entre otros, del calendario de entrega de documentación relativa a la definición de procesos, hitos destacables, dedicación por parte de BFA-DFB y propia.

La empresa adjudicataria se responsabilizará asimismo de la elaboración de la documentación de soporte para las sesiones de formación en coordinación con la Sección de Asesoramiento Jurídico, Seguridad de la Información y Protección de Datos, y el Servicio de Formación de la Diputación Foral de Bizkaia.



3.2 LOTE 2: SERVICIO DE DPO PARA LAS ENTIDADES LOCALES DEL TERRITORIO HISTÓRICO DE BIZKAIA (GRUPO 1)

Consistirá en prestar a la Entidad el servicio de Delegada/o de Protección de Datos (en adelante DPO), con las competencias y responsabilidades que la normativa asigna a este rol.

Las organizaciones públicas deben incorporar una persona DPO. La adjudicataria colaborará con la entidad local para elaborar una propuesta de designación y notificarlo a la agencia de control correspondiente una vez adoptada la decisión.

La entidad local es responsable de adoptar la decisión y de publicar la información relativa a este rol.

La persona designada DPO participará en cumplimiento de sus funciones en la fase de adecuación de la entidad local.

Para una gestión y coordinación adecuada de los datos personales de la organización, es necesaria la incorporación de la figura del DPO. La figura del DPO tiene como objetivos la información, la supervisión del cumplimiento, el asesoramiento y la cooperación respecto del cumplimiento de la normativa de protección de datos.

3.2.1 Servicio de Delegada/o de Protección de Datos (DPO)

Se desarrollarán las funciones definidas en el Art. 39 del RGPD

- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento, de las obligaciones del RGPD y demás normativa aplicable en protección de datos.
- Supervisar el cumplimiento del RGPD y demás normativa aplicable en protección de datos, y de las políticas del responsable o encargado del tratamiento en dicha materia, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en operaciones de tratamiento, y las auditorías correspondientes.
- Ofrecer el asesoramiento que se solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación conforme al Art. 35 del RGPD.
- Cooperar con la autoridad de control. Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa del artículo 36 del RGPD, y realizar consultas, en su caso, sobre cualquier otro asunto.
- Participar en las decisiones relativas al diseño de los tratamientos de datos personales, en lo que al cumplimiento del Reglamento se refiere.

Resultados:

Como resultado del cumplimiento de sus funciones, la persona DPO entregará a la Entidad:

- Por cada actuación realizada, un informe que contenga, al menos, el objeto de la actuación (consulta de la entidad, reclamación de persona interesada, de una agencia de control, incidencia, etc.), descripción del asunto tratado, las conclusiones y su fundamento. Se adjuntará cualquier otra información relevante que se haya utilizado durante la actuación.



Si durante la actuación, fuera necesario que la persona DPO accediera a datos de personas interesadas, una vez finalizada la actuación destruirá toda la información que le haya sido entregada (salvo referencias que pueda haber en el informe entregado). La entidad será responsable de conservar la información que sea necesaria.

- Al finalizar el servicio (o al menos, anualmente) un sumario con las actuaciones solicitadas, finalizadas y pendientes.

Para la prestación del servicio de DPO se deben dar unas condiciones mínimas que garanticen el éxito de sus funciones.

- La entidad facilitará a la persona DPO apoyo activo en su labor desde el máximo órgano de decisión, de manera que tenga capacidad suficiente para requerir la información y para promover las acciones de corrección necesarias en el ámbito de su actuación.
- La entidad realizará la comunicación oficial de la designación de la persona DPO a todo el personal para garantizar que su existencia y función se conozcan dentro de la organización.
- La entidad facilitará el acceso a las áreas o departamentos necesarios (recursos humanos, departamento jurídico, TI, seguridad, etc.) de modo que la persona DPO puedan recibir apoyo esencial, aportaciones e información de dichos servicios en el ámbito del cumplimiento de sus funciones.
- La entidad facilitará que la persona DPO tenga capacidad de intervenir en el diseño y supervisión de las actividades de tratamiento de datos personales, de modo que pueda aportar sus recomendaciones orientadas a garantizar el cumplimiento.

3.2.2 Descripción y detalle del servicio relativo a formación. La adjudicataria llevará a cabo sesiones formativas dirigidas al personal de la entidad y orientadas a la formación y concienciación en los principios del RGPD y LOPD-GDD en lo relativo al tratamiento de datos. Las sesiones de formación dirigidas al personal de las entidades locales serán como mínimo 4. La formación deberá proporcionar contenidos teóricos y eminentemente prácticos para la implementación de los procesos definidos para la adecuación al RGPD y LOPD-GDD.

3.3 LOTE 3: SERVICIO DE DPO PARA LAS ENTIDADES LOCALES DEL TERRITORIO HISTÓRICO DE BIZKAIA (GRUPO 2)

Consistirá en prestar a la entidad el servicio de Delegada/o de Protección de Datos (en adelante DPO), con las competencias y responsabilidades que la normativa asigna a este rol.

Las organizaciones públicas deben incorporar una persona DPO. La adjudicataria colaborará con la entidad local para elaborar una propuesta de designación y notificarlo a la agencia de control correspondiente una vez adoptada la decisión.

La entidad local es responsable de adoptar la decisión y de publicar la información relativa a este rol.



La persona designada DPO participará en cumplimiento de sus funciones en la fase de adecuación de la entidad local.

Para una gestión y coordinación adecuada de los datos personales de la organización, es necesaria la incorporación de la figura del DPO. La figura del DPO tiene como objetivos la información, la supervisión del cumplimiento, el asesoramiento y la cooperación respecto del cumplimiento de la normativa de protección de datos.

3.3.1 Servicio de Delegada/o de Protección de Datos (DPO)

Se desarrollarán las funciones definidas en el Art. 39 del RGPD

- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento, de las obligaciones del RGPD y demás normativa aplicable en protección de datos.
- Supervisar el cumplimiento del RGPD y demás normativa aplicable en protección de datos, y de las políticas del responsable o encargado del tratamiento en dicha materia, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en operaciones de tratamiento, y las auditorías correspondientes.
- Ofrecer el asesoramiento que se solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación conforme al Art. 35 del RGPD.
- Cooperar con la autoridad de control. Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa del artículo 36 del RGPD, y realizar consultas, en su caso, sobre cualquier otro asunto.
- Participar en las decisiones relativas al diseño de los tratamientos de datos personales, en lo que al cumplimiento del Reglamento se refiere.

Resultados:

Como resultado del cumplimiento de sus funciones, la persona DPO entregará a la entidad:

- Por cada actuación realizada, un informe que contenga, al menos, el objeto de la actuación (consulta de la entidad, reclamación de persona interesada, de una agencia de control, incidencia, etc.), descripción del asunto tratado, las conclusiones y su fundamento. Se adjuntará cualquier otra información relevante que se haya utilizado durante la actuación.
Si durante la actuación, fuera necesario que la persona DPO accediera a datos de personas interesadas, una vez finalizada la actuación destruirá toda la información que le haya sido entregada (salvo referencias que pueda haber en el informe entregado). La entidad será responsable de conservar la información que sea necesaria.
- Al finalizar el servicio (o al menos, anualmente) un sumario con las actuaciones solicitadas, finalizadas y pendientes.

Para la prestación del servicio de DPO se deben dar unas condiciones mínimas que garanticen el éxito de sus funciones.



- La entidad facilitará a la persona DPO apoyo activo en su labor desde el máximo órgano de decisión, de manera que tenga capacidad suficiente para requerir la información y para promover las acciones de corrección necesarias en el ámbito de su actuación.
- La entidad realizará la comunicación oficial de la designación de la persona DPO a todo el personal para garantizar que su existencia y función se conozcan dentro de la organización.
- La entidad facilitará el acceso a las áreas o departamentos necesarios (recursos humanos, departamento jurídico, TI, seguridad, etc.) de modo que la persona DPO puedan recibir apoyo esencial, aportaciones e información de dichos servicios en el ámbito del cumplimiento de sus funciones.
- La entidad facilitará que la persona DPO tenga capacidad de intervenir en el diseño y supervisión de las actividades de tratamiento de datos personales, de modo que pueda aportar sus recomendaciones orientadas a garantizar el cumplimiento.

3.3.2 Descripción y detalle del servicio relativo a formación. La adjudicataria llevará a cabo sesiones formativas dirigidas al personal de la entidad y orientadas a la formación y concienciación en los principios del RGPD y LOPD-GDD en lo relativo al tratamiento de datos. Las sesiones de formación dirigidas al personal de las entidades locales serán como mínimo 4. La formación deberá proporcionar contenidos teóricos y eminentemente prácticos para la implementación de los procesos definidos para la adecuación al RGPD y LOPD-GDD.

3.4 LOTE 4: SERVICIOS ORIENTADOS A LA ADECUACIÓN DE LAS ENTIDADES LOCALES DEL TERRITORIO HISTÓRICO DE BIZKAIA AL RGPD Y A LA LOPD-GDD (GRUPO 3)

3.4.1. Asesoramiento jurídico-técnico a la Entidad. Apoyo presencial, telefónico y telemático a demanda. En concreto:

- ✓ Resolución de dudas y consultas de índole jurídica, organizativa o técnica relacionadas con la materia de protección de datos.
- ✓ Revisión, actualización y propuesta de elaboración de cláusulas o avisos legales, así como de otros documentos o informes relacionados.
- ✓ Elaboración y redacción de la documentación necesaria en materia de política de privacidad.
- ✓ Revisión, actualización y propuesta de elaboración de contratos de acceso a datos (así como otras prestaciones de servicios sin acceso a datos pero que se vean afectadas por lo dispuesto en el RGPD y la Ley Orgánica 3/2018).
- ✓ Colaboración con la persona DPO en la coordinación, gestión y control de los procedimientos de Seguridad (incidencias, administración de usuarios, ejercicio de derechos acceso, rectificación, supresión, limitación del tratamiento, portabilidad y oposición.), gestión de soportes, accesos a dependencias, etc.),



- ✓ Asesoramiento, y elaboración de propuestas de informes y documentación ante posibles denuncias ante las Autoridades de Control en materia de protección de datos.

Para la prestación del servicio, a demanda de la entidad local, la empresa adjudicataria garantizará:

- Asistencia a reuniones internas de seguimiento y de impulso de los trabajos emprendidos. Las reuniones se planificarán en colaboración con la entidad local.
- Preparación y asistencia a reuniones con otros organismos, al objeto de prestar apoyo directo, como asesores jurídicos, a los responsables de la entidad ante dichos organismos.
- Elaboración de toda la documentación derivada de dichas reuniones, así como el envío de la citada información a la entidad en el formato que determine la entidad local.

3.4.2. Servicio de consultoría para la adecuación de la Entidad al RGPD y a la LOPD-GDD:

- ✓ Análisis de tratamientos y elaboración del Registro de Actividades de Tratamiento, así como la información que aporten los interlocutores, se identificarán y analizarán los tratamientos y flujos de datos personales de la entidad y se elaborará el Registro adecuado a la entidad según lo requerido.
- ✓ Análisis de riesgos. La Adjudicataria analizará junto con la entidad los riesgos en los tratamientos. Como resultado, se obtendrá información relativa a qué riesgos afectan a los tratamientos, de cara a establecer un plan de Tratamiento de Riesgos de mejora o de reducción de riesgos.

En este análisis se revisarán procesos internos tales como

- El diseño de los tratamientos, de manera que se asegure la protección de los datos. Esto incluye aspectos como medios técnicos y humanos que intervienen en el tratamiento, procedimientos de trabajo, intercambios.
- Los procedimientos de ejercicio de derechos de interesados.
- Riesgos en infraestructuras TIC que soportan los tratamientos.
- Los procedimientos para detectar y gestionar incidencias de seguridad, identificar las que puedan producir fugas de información y las obligaciones al respecto.
- Las condiciones de contratación a terceros, cuando implican acceso o tratamiento de los datos personales.
- Posibles transferencias internacionales de datos y sus condiciones.
- Las medidas de seguridad existentes.

Como resultado, se obtendrá un informe detallando qué riesgos afectan a los tratamientos, de cara a establecer un plan de mejora o de reducción de riesgos de tratamiento de riesgos

Evaluaciones de Impacto

- ✓ La adjudicataria elaborará el estudio preliminar de los tratamientos para determinar si es necesario realizar la evaluación de impacto en la privacidad. En el caso que se detecte que alguno de los tratamientos de datos personales genera un alto riesgo para los derechos y libertades de los interesados, se debe elaborar una evaluación de impacto relativa a la protección de datos para cada uno de ellos. En caso negativo, se redactará y registrará la justificación de la no necesidad de evaluación de impacto.



- ✓ Procedimientos de ejercicio de derechos. La adjudicataria asesorará a la entidad en el establecimiento de mecanismos visibles, accesibles y sencillos, incluidos los medios electrónicos, para el ejercicio de derechos y en el establecimiento de procedimientos que permitan responder a los ejercicios de derechos en los plazos previstos.
- ✓ Plan de mejora. La adjudicataria elaborará un Plan de mejora de Tratamientos de Riesgos para la entidad. En este Plan, deben priorizarse las medidas orientadas a mitigar riesgos en tratamientos que conlleven un mayor riesgo de lesionar derechos y las libertades de los interesados, en función de la sensibilidad de los datos, del ámbito en que se realiza el tratamiento y del volumen de datos tratados.

El Plan recogerá, al menos:

- Criterios o decisiones a adoptar por la entidad necesarios para el Registro de tratamientos. Por ejemplo, decisiones relativas a la legitimidad de los tratamientos, identificación de la legislación que justifique el tratamiento, de los criterios o plazos de supresión; necesidades de recabar consentimientos para tratamientos donde no se haya conservado esta información, etc. Este tipo de actuaciones por parte de la entidad se incluirán en el Plan como tareas detalladas dentro del Plan de mejora.
 - Diseño de las modificaciones necesarias en los tratamientos existentes, allá donde se detecten riesgos o carencias.
 - Modificaciones necesarias en los procedimientos de ejercicio de derechos, cláusulas de información, de contratos con proveedores, plazos o formas de ejercer derechos, notificaciones, etc.
 - Modificaciones en los procedimientos de gestión de incidencias y notificación de brechas.
 - Modificaciones en las condiciones de contratación de proveedores.
 - Modificaciones en las condiciones de transferencias internacionales.
 - Diseño de otras medidas de seguridad tanto técnicas como organizativas que eviten la pérdida de información, la destrucción involuntaria de datos o el acceso de un tercero no autorizado, y que a su vez garanticen la integridad, la disponibilidad y la inalterabilidad de los datos tratados.
- ✓ Acreditar el cumplimiento. La adjudicataria entregará a la entidad un expediente con documentación final que le permita demostrar que los tratamientos de datos personales se realizan cumpliendo con la normativa y se aplican las medidas técnicas y organizativas correspondientes.

El expediente deberá contener al menos los siguientes elementos:

Documentación, Procedimientos de seguridad y Registros de:

- Análisis de riesgos: documentación de la metodología, tareas realizadas y resultados.
- Evaluaciones de impacto sobre la privacidad: documentación de la metodología utilizada y resultados de la evaluación incluida la justificación de la no necesidad de evaluación para ciertos tratamientos cuando sea necesario.
- Procedimientos relativos al ejercicio de derechos en materia de protección de datos.
 - documentos de información al interesado.
 - procedimientos y formularios para el ejercicio de los derechos de las personas en materia de protección de datos.



- Modelo de Registro de registro de solicitudes de ejercicio de derechos de personas interesadas y de respuestas para dichas solicitudes.
- Modelos de contratos con los encargados del tratamiento aplicables en las contrataciones.
- Procedimiento de gestión de incidencias.
- Procedimiento de control de acceso a la información.
- Modelos de Registro de Incidencias, de control de acceso a la información.
- Documentación de posibles transferencias internacionales de datos.
- Documentación de apoyo a la Formación en la entidad:
 - A los roles con responsabilidad en los Servicios/Tratamientos.
 - A todo el personal de la entidad.

3.4.3 Sesiones formativas:

La adjudicataria llevará a cabo sesiones formativas dirigidas al personal de la entidad y orientadas a la formación y concienciación en los principios del Reglamento en lo relativo al tratamiento de datos. Las sesiones de formación dirigidas a las entidades locales serán como mínimo 4. La formación deberá proporcionar contenidos teóricos y eminentemente prácticos para la implementación de los procesos definidos para la adecuación al RGPD y LOPD-GDD.

3.5 LOTE 5: SERVICIOS ORIENTADOS A LA ADECUACIÓN DE LAS ENTIDADES LOCALES DEL TERRITORIO HISTÓRICO DE BIZKAIA AL RGPD Y A LA LOPD-GDD (GRUPO 4)

3.5.1. Asesoramiento jurídico-técnico a la Entidad. Apoyo presencial, telefónico y telemático a demanda. En concreto:

- ✓ Resolución de dudas y consultas de índole jurídica, organizativa o técnica relacionadas con la materia de protección de datos.
- ✓ Revisión, actualización y propuesta de elaboración de cláusulas o avisos legales, así como de otros documentos o informes relacionados.
- ✓ Elaboración y redacción de la documentación necesaria en materia de política de privacidad.
- ✓ Revisión, actualización y propuesta de elaboración de contratos de acceso a datos (así como otras prestaciones de servicios sin acceso a datos pero que se vean afectadas por lo dispuesto en el RGPD y la Ley Orgánica 3/2018).
- ✓ Colaboración con la persona DPO en la coordinación, gestión y control de los procedimientos de Seguridad (incidencias, administración de usuarios, ejercicio de derechos acceso, rectificación, supresión, limitación del tratamiento, portabilidad y oposición.), gestión de soportes, accesos a dependencias, etc.).



- ✓ Asesoramiento, y elaboración de propuestas de informes y documentación ante posibles denuncias ante las Autoridades de Control en materia de protección de datos.

Para la prestación del servicio, a demanda de la entidad local, la empresa adjudicataria garantizará:

- Asistencia a reuniones internas de seguimiento y de impulso de los trabajos emprendidos. Las reuniones se planificarán en colaboración con la entidad local.
- Preparación y asistencia a reuniones con otros organismos, al objeto de prestar apoyo directo, como asesores jurídicos, a los responsables de la entidad ante dichos organismos.
- Elaboración de toda la documentación derivada de dichas reuniones, así como el envío de la citada información a la entidad en el formato que determine la entidad local.

3.5.2. Servicio de consultoría para la adecuación de la Entidad al RGPD y a la LOPD-GDD:

- ✓ Análisis de tratamientos y elaboración del Registro de Actividades de Tratamiento así como la información que aporten los interlocutores, se identificarán y analizarán los tratamientos y flujos de datos personales de la entidad y se elaborará el Registro adecuado a la entidad según lo requerido.
- ✓ Análisis de riesgos. La Adjudicataria analizará junto con la entidad los riesgos en los tratamientos. Como resultado, se obtendrá información relativa a qué riesgos afectan a los tratamientos, de cara a establecer un plan de Tratamiento de Riesgos de mejora o de reducción de riesgos.

En este análisis se revisarán procesos internos tales como

- El diseño de los tratamientos, de manera que se asegure la protección de los datos. Esto incluye aspectos como medios técnicos y humanos que intervienen en el tratamiento, procedimientos de trabajo, intercambios.
- Los procedimientos de ejercicio de derechos de interesados.
- Riesgos en infraestructuras TIC que soportan los tratamientos.
- Los procedimientos para detectar y gestionar incidencias de seguridad, identificar las que puedan producir fugas de información y las obligaciones al respecto.
- Las condiciones de contratación a terceros, cuando implican acceso o tratamiento de los datos personales.
- Posibles transferencias internacionales de datos y sus condiciones.
- Las medidas de seguridad existentes.

Como resultado, se obtendrá un informe detallando qué riesgos afectan a los tratamientos, de cara a establecer un plan de mejora o de reducción de riesgos de tratamiento de riesgos.

Evaluaciones de Impacto

- ✓ La adjudicataria elaborará el estudio preliminar de los tratamientos para determinar si es necesario realizar la evaluación de impacto en la privacidad. En el caso que se detecte que alguno de los tratamientos de datos personales genera un alto riesgo para los derechos y libertades de los interesados, se debe elaborar una evaluación de impacto relativa a la protección de datos para cada uno de ellos. En caso negativo, se redactará y registrará la justificación de la no necesidad de evaluación de impacto.



- ✓ Procedimientos de ejercicio de derechos. La adjudicataria asesorará a la entidad en el establecimiento de mecanismos visibles, accesibles y sencillos, incluidos los medios electrónicos, para el ejercicio de derechos y en el establecimiento de procedimientos que permitan responder a los ejercicios de derechos en los plazos previstos.
- ✓ Plan de mejora. La adjudicataria elaborará un Plan de mejora de Tratamientos de Riesgos para la entidad. En este Plan, deben priorizarse las medidas orientadas a mitigar riesgos en tratamientos que conlleven un mayor riesgo de lesionar derechos y las libertades de los interesados, en función de la sensibilidad de los datos, del ámbito en que se realiza el tratamiento y del volumen de datos tratados.

El Plan recogerá, al menos:

- Criterios o decisiones a adoptar por la entidad necesarios para el Registro de tratamientos. Por ejemplo, decisiones relativas a la legitimidad de los tratamientos, identificación de la legislación que justifique el tratamiento, de los criterios o plazos de supresión; necesidades de recabar consentimientos para tratamientos donde no se haya conservado esta información, etc. Este tipo de actuaciones por parte de la entidad se incluirán en el Plan como tareas detalladas dentro del Plan de mejora.
 - Diseño de las modificaciones necesarias en los tratamientos existentes, allá donde se detecten riesgos o carencias.
 - Modificaciones necesarias en los procedimientos de ejercicio de derechos, cláusulas de información, de contratos con proveedores, plazos o formas de ejercer derechos, notificaciones, etc.
 - Modificaciones en los procedimientos de gestión de incidencias y notificación de brechas.
 - Modificaciones en las condiciones de contratación de proveedores.
 - Modificaciones en las condiciones de transferencias internacionales.
 - Diseño de otras medidas de seguridad tanto técnicas como organizativas que eviten la pérdida de información, la destrucción involuntaria de datos o el acceso de un tercero no autorizado, y que a su vez garanticen la integridad, la disponibilidad y la inalterabilidad de los datos tratados.
- ✓ Acreditar el cumplimiento. La adjudicataria entregará a la entidad un expediente con documentación final que le permita demostrar que los tratamientos de datos personales se realizan cumpliendo con la normativa y se aplican las medidas técnicas y organizativas correspondientes.

El expediente deberá contener al menos los siguientes elementos:

Documentación, Procedimientos de seguridad y Registros de:

- Análisis de riesgos: documentación de la metodología, tareas realizadas y resultados.
- Evaluaciones de impacto sobre la privacidad: documentación de la metodología utilizada y resultados de la evaluación incluida la justificación de la no necesidad de evaluación para ciertos tratamientos cuando sea necesario.
- Procedimientos relativos al ejercicio de derechos en materia de protección de datos.
 - documentos de información al interesado.
 - procedimientos y formularios para el ejercicio de los derechos de las personas en materia de protección de datos.



- Modelo de Registro de registro de solicitudes de ejercicio de derechos de personas interesadas y de respuestas para dichas solicitudes.
- Modelos de contratos con los encargados del tratamiento aplicables en las contrataciones.
- Procedimiento de gestión de incidencias.
- Procedimiento de control de acceso a la información.
- Modelos de Registro de Incidencias, de control de acceso a la información.
- Documentación de posibles transferencias internacionales de datos.
- Documentación de apoyo a la Formación en la entidad:
 - A los roles con responsabilidad en los Servicios/Tratamientos.
 - A todo el personal de la entidad.

3.5.3 Sesiones formativas:

La adjudicataria llevará a cabo sesiones formativas dirigidas al personal de la entidad y orientadas a la formación y concienciación en los principios del Reglamento en lo relativo al tratamiento de datos. Las sesiones de formación dirigidas a las entidades locales serán como mínimo 4. La formación deberá proporcionar contenidos teóricos y eminentemente prácticos para la implementación de los procesos definidos para la adecuación al RGPD y LOPD-GDD.

4.CONDICIONES GENERALES

4.1 PARA EL LOTE 1

DFB facilitará el acceso a la plataforma tecnológica de gestión del RGPD que tenga homologada y en uso la DFB y el Sector Público Foral en el momento de la ejecución de las tareas por parte de la empresa adjudicataria.

Los trabajos se desarrollarán en los locales de la empresa contratada mediante conexión con los ordenadores de Lantik. En su caso los equipos, y comunicaciones que fueran necesarios para el acceso a la plataforma mencionada (incluso con la red de DFB) serán a cargo de la empresa contratada.

4.2 PARA LOS LOTES 2,3,4 y 5:

La adecuación se plantea desde el punto de vista de que muchas de las entidades participantes son ayuntamientos y entes municipales que cuentan con situaciones similares en cuanto a estructura, servicios prestados, tipos de datos que tratan, etc. Por lo tanto, en la propuesta metodológica se valorará el diseño de un esquema de adecuación general, aplicable a un grupo amplio de entidades, que pueda ser luego adaptado en cada caso.



La adjudicataria garantizará que las personas que intervienen en la prestación del servicio de DPO no participan en labores de adecuación al RGPD o, de forma más general, en labores de consultoría o asesoramiento en materia de seguridad.

4.3 PARA TODOS LOS LOTES

El material escrito a entregar deberá estar redactado en euskera y castellano. Se facilitará al menos una copia en papel y una copia electrónica en formato electrónico y editable. Cuando la naturaleza del contenido lo permita (inventarios y registros, listados, etc.) se entregarán formatos estructurados (hoja de cálculo, base de datos, ...) en lugar de documentos de texto, de cara a facilitar su manejo e integración con otras aplicaciones.

El personal a cargo de las tareas de adecuación y de prestar el servicio de DPO deberá tener capacidad de comunicarse en euskera y castellano.

5. CLÁUSULA DE IGUALDAD

Las empresas licitadoras, en la elaboración y presentación de sus respectivas propuestas deberán hacer un uso no sexista del lenguaje.

Asimismo, la empresa adjudicataria a lo largo de la vigencia del contrato deberá hacer un uso no sexista del lenguaje en cualquier documento definitivo escrito o digital, así como, deberá desagregar los datos por sexo en cualquier estadística referida a personas que se genere, todo ello al amparo del artículo 2.3 de la Ley 4/2005, de 18 de febrero, para la Igualdad de Mujeres y Hombres en el que se señalan los principios generales que deberán respetarse.

La empresa adjudicataria incluirá en la justificación final de realización de la prestación una memoria sobre el impacto de género de la contratación, con los indicadores y datos desagregados por sexo de las personas usuarias o beneficiarias, y del personal prestador del servicio, que posibiliten evaluar la eficacia de las medidas de igualdad aplicadas.

Sin./Fdo.: IZASKUN FURONES SIERRA - 2020-07-01
LEGE AHOLK., INFORM.SEGURTAS. ETA DATU BABESA BIDER.ATAL.BUR.
JEFE/A SECCIÓN DE ASESOR.JURÍD., SEGUR.INFORM.Y PROTEC.DATOS

Sin./Fdo.: LEIRE BEGOÑA VITORICA DONEZAR - 2020-07-03
GOBERNAMENDU ONERAKO ETA GARDENTASUNERAKO ZUZENDARITZA NAGUS-REN ZUZENDARI NAGUSIA
DIRECTOR/A GENERAL DE DIRECCIÓN GENERAL DE BUEN GOBIERNO Y TRANSPARENCIA



ANEXO: “TRATAMIENTO DE DATOS PERSONALES”

- **Finalidad:**

El tratamiento consistirá en la prestación del servicio de asistencia jurídica, organizativa y técnica en materia de protección de datos a la Diputación Foral de Bizkaia, entidades forales y entidades locales.

Para proporcionar los servicios establecidos en el Pliego, el personal adscrito a las empresas que resulten adjudicatarias pueden tratar datos personales. Los datos personales se tratarán únicamente por el personal adscrito y al único fin de efectuar el alcance contratado.

- **Legitimación del tratamiento:**

1. Art 28 RGPD
2. Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público.
3. Acuerdo marco de asesoramiento jurídico y de medidas técnicas y organizativas en materia de protección de datos.

- **Categorías de datos personales**

Datos identificativos y datos de contacto: nombre y apellidos, teléfono, correo electrónico, sexo, puesto de trabajo.

- **Descripción de las categorías de personas interesadas:**

- Personas beneficiarias
- Personas representantes legales
- Personas trabajadoras

- **Actividades del tratamiento**

Consulta de datos y copias temporales de datos.

- **Origen de los datos:**

Administración o entidad pública a la que se adjudique el contrato derivado.