



▶ ARABAKO FORU ALDUNDIA



Gizarte Ongizaterako
Foru Erakundea
Instituto Foral
De Bienestar Social

▶ DIPUTACIÓN FORAL DE ÁLAVA

Antetítulo informe

| Acuerdo para la adecuación de la Estructura Funcional de Seguridad del Instituto Foral de Bienestar Social de Álava a la nueva normativa de Protección de Datos



Control de versión

| VERSIÓN | FECHA | MOTIVO DEL CAMBIO |
|---------|------------|-------------------|
| 00 | 22/05/2019 | Versión inicial |

REALIZADO Y REVISADO

Firmado: VADILLO ASESORES SOLUCIONES JURÍDICAS A EMPRESAS, S.L.

Fecha: 22/05/2019

APROBADO

Aprobado por
DIRECCIÓN GERENCIA DEL IFBS

Firmado:

Fecha:



ÍNDICE

| | | |
|-----|--|---|
| 1 | Propuesta de Acuerdo de Estructura Funcional de Seguridad del IFBS | 4 |
| 1.1 | Contenido del Acuerdo | 4 |
| 1.2 | Anexo I | 8 |

1 Propuesta de Acuerdo de Estructura Funcional de Seguridad del IFBS

1.1 Contenido del Acuerdo

Estructura funcional para el tratamiento de Datos Personales del Instituto Foral de Bienestar Social, de acuerdo con el Reglamento Europeo General de Protección de Datos 2016/679 y la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales.

- I. El Reglamento Europeo General de Protección de Datos, Reglamento 2016/679, de 27 de abril, del Parlamento Europeo y del Consejo, 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 (en adelante RGPD), fue publicado el 4 de mayo de 2016, entrando en vigor ese mismo mes y siendo de aplicación a partir del 25 de mayo de 2018.

Dicho Reglamento es de aplicación directa en los distintos Estados miembros en virtud de lo dispuesto en el artículo 288 del Tratado de Funcionamiento de la Unión Europea, sin necesidad de ser transpuesto a la legislación nacional. No obstante, el 1 de diciembre de 2018 fue aprobada la Ley Orgánica 2/2018, de Protección de Datos Personales y garantía de los derechos digitales. (LOPDGDD).

Esta nueva normativa, además de desplazar a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y su Reglamento de desarrollo, introduce una serie de cambios en cuanto al enfoque de la materia, evolucionando de un modelo basado en el control del cumplimiento a otro basado en la responsabilidad activa, que consiste en garantizar el cumplimiento diligente y efectivo de la normativa y ser capaz de demostrarlo. Se pasa así de un sistema formalista y cerrado a un sistema abierto de gestión de riesgos basado en la prevención y que exige anticiparse a la infracción.

El Instituto Foral de Bienestar Social ha adquirido el compromiso de adaptar sus normas, procedimientos, y buenas prácticas a esta nueva normativa, así como de dotarse de forma paulatina de los recursos adecuados a las necesidades del tratamiento de la información, con el objeto de garantizar la seguridad de la información y el cumplimiento de la normativa sobre protección de datos.

Entre los elementos centrales de este nuevo marco jurídico se encuentra la obligación de las Administraciones públicas que traten datos personales de designar un Delegado de Protección de Datos, para lo cual a través de un acuerdo del Instituto Foral de Bienestar publicado en el Botha Núm. 127, de 05/11/2018., se designó a la empresa “VADILLO ASESORES SOLUCIONES JURÍDICAS A EMPRESAS, S.L.” como órgano unipersonal para el desarrollo de las funciones y competencias del cargo.

- II. Según la Ley Orgánica 3/2018) y el Reglamento (UE) 2016/679, el Instituto Foral de Bienestar Social determinará las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme a la legislación, entre las que se incluye la valoración sobre la realización de la evaluación de impacto en la protección de datos.
- III. En los términos fijados dicha normativa se establecen los siguientes roles funcionales:
- a) Responsable del tratamiento, responsable es el Instituto de Bienestar Social, de acuerdo con el art. 4.8 RGPD: *“la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros”*
 - b) Encargado del tratamiento o encargado es *“la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del Instituto de Bienestar Social de Álava”*.
Los responsables y encargados, teniendo en cuenta los elementos enumerados en los artículos 24 y 25 del Reglamento (UE) 2016/679, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el citado reglamento, con la presente ley orgánica, sus normas de desarrollo y la legislación sectorial aplicable (Art. 28 LOPDGD).
 - c) Delegado de Protección de Datos es *“quien, entre otras funciones, tiene las funciones de supervisar el cumplimiento de la normativa en materia de protección de datos personales y, en su caso, de gestionar las consultas de las personas que se pongan en contacto con el mismo en relación con el tratamiento de sus datos personales.”* (Art. 39 RGPD)

El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones. No será destituido ni sancionado por el Instituto Foral de Bienestar Social o el encargado por desempeñar sus funciones. El delegado de protección de datos rendirá cuentas directamente al más alto nivel jerárquico del IFBS o encargado. (Art. 38.3 RGPD)

El IFBS tiene que designar un delegado de protección de datos ya que: a) el tratamiento lo lleva a cabo una autoridad u organismo público (Art. 37.1 RGPD).

El delegado de protección de datos podrá formar parte de la plantilla del IFBS o desempeñar sus funciones en el marco de un contrato de servicios. (Art. 37.6 RGPD)

Los interesados podrán ponerse en contacto con el delegado de protección de datos por lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos al amparo del presente Reglamento. (Art. 38. 4 RGPD)

- IV. Además de los puestos funcionales definidos en el apartado II anterior, por razones de mayor operatividad se mantienen los siguientes roles de seguridad definidos específicamente del marco institucional del Instituto Foral de Bienestar Social.

El Instituto Foral de Bienestar Social podrá asistirse de los Responsables Funcionales de Tratamiento, es decir, de los Responsables de las Subdirecciones Técnicas que gestionan las actividades de tratamiento en su respectivo ámbito de actuación.

- V. Tanto los puestos funcionales definidos en los apartados II y III anteriores como el personal al servicio del Instituto Foral de Bienestar Social tratarán la información a que accedan en el desarrollo de sus funciones en los términos establecidos en la normativa legal correspondiente.

La descripción genérica de las funciones y roles indicados en los puntos anteriores se añade en lo que no contradiga y sustituye en caso contrario, a las que hasta el momento tenían encomendadas en relación con el tratamiento y la protección de datos cada uno de los puestos estructurales implicados en la gestión de los datos afectados por la anterior LOPD, por lo que no resulta preciso incrementar la plantilla de personal.

Dichas funciones se detallan en el documento titulado “Resumen de las Funciones y Obligaciones del Personal del Instituto Foral de Bienestar Social en relación con la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales”, que se adjunta como Anexo I al presente documento.

Por ello, este organismo considera oportuno actualizar la estructura funcional de seguridad y privacidad establecida con arreglo a la anterior LOPD, conforme a la actual normativa, de modo que garantice, regule y controle el tratamiento de la información a la que alude la LOPDGD y el RGPD.

En su virtud, a propuesta de la Dirección Gerencia y previa deliberación del Consejo de Administración del Instituto foral de Bienestar Social, en sesión celebrada por el mismo en el día de hoy,

ACUERDO

Primero. Designar al Instituto Foral de Bienestar Social como Responsable del Tratamiento, correspondiendo a la Dirección Gerencia el ejercicio de las funciones atribuidas al mismo.

Segundo. Designar Responsables de Tratamiento Funcionales internos a los Responsables de las Subdirecciones Técnicas de las actividades de tratamiento que gestionen en su respectivo ámbito de actuación, los cuales podrán ayudarse del personal operativo que consideren.

Tercero. Designar como Responsable de Seguridad de los tratamientos de esta Administración al Responsable de la Subdirección Técnica de Organización e Informática, o a la persona que esté designe en su defecto.

Cuarto. Por Acuerdo del Instituto Foral de Bienestar Social, publicado en el BOTHA Núm. 127 de 5 de noviembre de 2018, se procede por este organismo foral a la designación de la entidad “VADILLO ASESORES SOLUCIONES JURÍDICAS A EMPRESAS, S.L.” como Delegado de Protección de Datos externo que desempeñará sus funciones en el marco de un contrato de servicios en virtud de la habilitación legal existente.

Quinto. Establecer las funciones y obligaciones del personal del Instituto Foral de Bienestar Social en relación con la Ley Orgánica de Protección de Datos de Personales y garantía de los derechos digitales, recogidas en el Anexo I a este Acuerdo.

Sexto. Este Acuerdo entrará en vigor al día siguiente de su publicación en el BOTHA.

En Vitoria-Gasteiz, a XX de Mayo de 2019. – La presidenta del Consejo de Administración, xxxxxx.

1.2 Anexo I

El presente Anexo al Acuerdo de Adecuación de la Estructura de Seguridad Funcional del IFBS a la normativa de Protección de Datos, describe las funciones y obligaciones del personal del instituto foral de bienestar social en relación con la Ley Orgánica de Protección de Datos Personales y Garantía de Derechos Digitales:

1. Funciones y obligaciones del Instituto Foral de Bienestar Social como Responsable del Tratamiento

Corresponde a la Dirección Gerencia del IFBS en su calidad de Responsable de Tratamiento, de acuerdo con el art. 24 RGPD y art. 28 LOPDGDD:

- a) Garantizar la protección de datos desde el diseño y por defecto, asegurando el cumplimiento de los principios de protección de datos;
- b) Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el IFBS aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar por defecto que el tratamiento es conforme con el presente Reglamento y que solo son objeto de tratamiento los datos personales necesarios para cada uno de los fines específicos del tratamiento. Dichas medidas se revisarán y actualizarán cuando sea necesario;
- c) Creación y mantenimiento actualizado del registro de actividades de tratamiento, y valoración, y realización en su caso, de la evaluación de impacto en la protección de datos;
- d) Determinación de la finalidad, contenido y uso del tratamiento de los datos afectados por la LOPDGD;
- e) Identificación de terceros Encargados de Tratamiento, por los Responsables Funcionales de los Tratamientos y al Responsable de Seguridad;
- f) Cumplimiento del deber de transparencia, así como del deber de atender los derechos de las personas interesadas en materia de protección de datos, estableciendo y gestionando procedimientos para la recepción, tramitación, seguimiento y atención de las solicitudes de derechos de acceso, supresión, rectificación, oposición, limitación, portabilidad, y a no ser objeto de decisiones automatizadas;
- g) Difusión y comunicación de buenas prácticas en materia de protección de datos personales implementadas en el seno de este organismo foral, formando y concienciando a todo el personal sobre las mismas;
- h) Adhesión a códigos de conducta aprobados a tenor del artículo 40 del RGPD, o a un mecanismo de certificación aprobado a tenor del artículo 42 RGPD, podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del IFBS.

2. Funciones y obligaciones de los Encargados del Tratamiento

Corresponde al Encargado del tratamiento de acuerdo con el art. 28 RGPD y el art. 33 LOPDGD:

- a) Seguir las instrucciones dadas por el Instituto Foral de Bienestar Social, inclusive en lo que respecta a las transferencias de datos personales a un tercer país o una organización internacional y a la posibilidad o prohibición de contratar, establecidas en virtud del correspondiente contrato o Convenio;
- b) Llevanza del registro de actividades del tratamiento, y efectuar el análisis de riesgos de cada tratamiento que efectúa por cuenta del IFBS, así como implantar las medidas de seguridad adecuadas a dicho tratamiento, garantizando la protección de la información proporcionalmente al tipo de tratamiento y al tipo de datos que conlleva la prestación del servicio realizada;
- c) Garantizar que las personas autorizadas para tratar datos personales se han comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria;
- d) Respetar las condiciones indicadas por el IFBS para recurrir a otro encargado del tratamiento, y en particular no recurrir a otro encargado sin la autorización previa por escrito, específica o general del IFBS, informándole de cualquier cambio previsto en la incorporación o sustitución de otros encargados, eligiendo únicamente encargados de tratamiento que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con la normativa;
- e) Asistir al IFBS, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, y ayudarle a cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados;
- f) A elección del IFBS, el Encargado suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros;
- g) Cooperación con la autoridad de control y puesta a disposición del IFBS toda la información necesaria para demostrar el cumplimiento de estas obligaciones, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del IFBS o de otro auditor autorizado por dicho responsable.

3. Funciones del Delegado de Protección de Datos

Corresponde al Delegado de Protección de Datos de acuerdo con el art.39 RGPD y el art. 37 LOPDGD:

- a) Desempeñar sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

- b) informar y asesorar al IFBS o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben, en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros
- c) supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del IFBS o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;
- d) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35;
- e) cooperar con la autoridad de control;
- f) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.
- g) interlocución e información con las personas interesadas, emisión de informes sobre las solicitudes de ejercicio de derechos cuando lo solicite el IFBS, así como la tramitación de las reclamaciones previas que interpongan las personas afectadas.

4. Funciones del Responsable de Seguridad

Son funciones del Responsable de Seguridad el cumplimiento de todos los aspectos determinados por la Ley Orgánica de Protección de Datos Personales y Garantía De Derechos Digitales, sobre la implantación de medidas de seguridad adecuadas a los riesgos que pesa sobre los tratamientos, de manera coordinada con los Responsable de Tratamiento:

- a) índole organizativa y técnica,
- b) normativa legal,
- c) control y gestión de la documentación exigida,
- d) actualización de las políticas y procedimientos de seguridad,
- e) Implantación de las medidas de seguridad necesarias, mecanismos de protección, y las oportunas políticas de protección de datos,
- f) Aprobación, difusión y comunicación de las prácticas de seguridad implementadas a los usuarios del interior de la organización, formando y concienciando a todo el personal sobre las mismas,
- g) Interlocución con el personal interno del organismo foral así como con las personas titulares de los datos o afectadas para la explicación de cuestiones técnicas, en su caso;

- h) Asesoramiento al IFBS y puesta a disposición de la información necesaria para la toma de decisiones por parte de los Responsables Funcionales de Tratamiento y del Delegado de Protección de Datos;
- i) Regularización en las relaciones con terceros (cesión de datos y acceso por cuenta de terceros), y elegir únicamente encargados de tratamiento que ofrezcan garantías suficientes,
- j) Coordinación en la implantación de medidas de verificación de cumplimiento y los controles periódicos y auditorías,
- k) Verificación de la recuperación de datos activos y de los datos históricos no accesibles,
- l) Aplicación de procedimientos de seguridad: gestión de incidencias, control y registro de accesos lógicos y físicos, copias de respaldo y recuperación, gestión de soportes, etc.
- m) Notificación al Responsable Funcional de Tratamiento y al DPD de cualquier incidencia o brecha de seguridad que tenga lugar y que afecte o pudiera afectar a los datos de carácter personal.

5. Funciones de los Responsables Funcionales de los Tratamientos

Son funciones de ejecución directa del Responsable Funcional del Tratamiento, las propias del Responsable de Tratamiento, y en concreto:

- a) Se encargarán de que el Registro de Actividades de Tratamiento se mantenga actualizado
- b) Se encargará de implantar las políticas, procedimiento y registros elaborados al efecto para el cumplimiento de la normativa, especialmente los referidos al cumplimiento del deber de transparencia, de consentimiento explícito y de ejercicio de derechos de las personas interesadas
- c) Coordinación con el Responsable de Seguridad y el DPD en la adopción de medidas apropiadas de índole organizativa y técnica;
- d) Toma de decisión para la aplicación de las medidas de seguridad necesarias, mecanismos de protección, y las oportunas políticas de protección de datos;
- e) Se encargarán de realizar acciones periódicas de formación y concienciación al personal en relación a la documentación y buenas prácticas de protección de datos personales que se vayan implementando en el seno de este organismo foral, formando y concienciando a todo el personal sobre las mismas;
- f) Realización de evaluaciones de impacto de los tratamientos de datos personales, y el análisis de riesgos, fundamentalmente en cuestiones organizativas y técnicas, solicitando el apoyo necesario al Responsable de Seguridad, al DPD así como a los Encargados de Tratamiento afectado en cada caso;
- g) Elección de encargados de tratamiento que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del RGPD,

- h) Toma de decisiones en relación a la gestión de las entradas y salidas de información en cualquier soporte, así como la gestión de accesos autorizados a la misma
- i) Toma de decisiones en relación a la supresión de datos bloqueados no activos ni accesibles
- j) Toma de decisiones en relación a la correcta gestión y custodia de soportes no automatizados
- k) Notificación al DPD acerca de cualquier incidencia o brecha de seguridad que pudiera tener lugar y que afecte o pudiera afectar a los datos de carácter personal o a la seguridad de la información.

6. Funciones del Delegado de Protección de Datos

Las funciones y obligaciones del Delegado de Protección de Datos se resumen en:

- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones del Reglamento y demás normativa aplicable en protección de datos.
- Supervisar el cumplimiento del Reglamento 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.
- 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, y realizar consultas, en su caso, sobre cualquier otro asunto.

Para ello, se deberá:

- Asegurar su participación en todos los asuntos relativos a la protección de datos.
- Proporcionarle los recursos necesarios para la realización de sus tareas.
- Garantizar que pueda actuar de forma independiente.
- Facilitar su acceso a los datos y operaciones de procesamiento.
- Comunicar oficialmente su designación.
- Permitir la formación continua