DOCUMENTO DE SEGURIDAD DE PROTECCIÓN DE DATOS

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos - RGPD)

Organización	MUGARIK GABE ORGANIZACIÓN NO GUBERNAMENTAL DE COOPERACIÓN AL DESARROLLO (ONGD)
NIF	G-48263446
Actividad	Cooperación internacional y Educación para la transformación
Domicilio	Gpo Vicente Garamendi 5, bajo 48006 Bilbao
Email:	Bilbao@mugarikgabe.org
Teléfono:	944154307
Responsable Privacidad	Susana Piera Moreno
Fecha DSPD	

Nº	MODIFICACIONES	FECHA APROBACIÓN	RESPONSABLE
0	Edición Inicial	15-03-2019	Susana Piera

ÍNDICE

1. INTRODUCCIÓN

El 26 de abril de 2016 la Unión Europea aprobó el Reglamento General de Protección de Datos (RGPD) que es de plena aplicación a partir del 25 de mayo de 2018.

La mayor innovación del RGPD respecto de las obligaciones establecidas para los responsables de tratamiento de datos descansa sobre dos premisas:

- Responsabilidad proactiva.
- Riesgo.

El principio de responsabilidad proactiva que se puede definir como la necesidad de que el responsable del tratamiento aplique medidas técnicas y organizativas apropiadas, a fin de garantizar y poder demostrar que el tratamiento de datos es conforme con la normativa vigente.

En términos prácticos, este principio requiere que las organizaciones analicen qué datos tratan, con qué finalidades lo hacen y qué tipo de operaciones de tratamiento llevan a cabo. A partir de este conocimiento deben determinar de forma explícita la forma en que aplicarán las medidas que el RGPD prevé, asegurándose de que esas medidas son las adecuadas para cumplir con el mismo y de que pueden demostrarlo ante los interesados y ante las autoridades de supervisión.

En síntesis, ahora se exige una actitud consciente, diligente y proactiva por parte de las organizaciones frente a todos los tratamientos de datos personales que lleven a cabo.

Además, el RGPD en función del riesgo señala que las medidas dirigidas a garantizar su cumplimiento deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como el riesgo para los derechos y libertades de las personas.

La aplicación de las medidas previstas por el RGPD debe adaptarse, por tanto, a las características de cada organización y sus circunstancias particulares.

1.1. Objeto del documento de seguridad

El RGPD indica que 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 responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento.

Este documento se elabora por **MUGARIK GABE ONGD**, como responsable de tratamiento y encargado en algunos casos, con la finalidad de uniformar las distintas medidas y procedimientos desarrollados para dar cumplimiento a la normativa de privacidad, con una actitud responsable y activa frente a todos los tratamientos de datos personales que lleva a cabo.

A su vez adquiere el compromiso de mantenerlo actualizado y de divulgarlo a todo el personal con acceso a los datos de carácter personal o a los sistemas de información que permiten el tratamiento de los mismos.

1.2. Ámbito de aplicación

El presente documento tiene como ámbito de aplicación:

- los tratamientos que contienen datos de carácter personal que se hallan bajo la responsabilidad **MUGARIK GABE ONGD** (bien como responsable o como encargado de tratamiento, en su caso),
- los sistemas de información, soportes y equipos empleados para el tratamiento de datos de carácter personal que deban ser protegidos de acuerdo a lo dispuesto en normativa vigente,
- las personas y puestos de trabajo que intervienen en el tratamiento,
- y los locales en los que se ubican.

1.3. Formato del documento de seguridad

El formato de este documento de seguridad es digital. En el mismo se desarrollan todas las obligaciones que la normativa de privacidad establece y que se completa con los siguientes anexos

- **Anexo 1_Interesados,** contiene los procedimientos, medidas y modelos de cláusulas informativas utilizados por **MUGARIK GABE ONGD** para informar al titular de los datos y para garantizar el ejercicio de sus derechos para que el tratamiento de los datos sea legítimo.

- **Anexo 2_Responsable_ Encargado de Tratamiento,** contiene los procedimientos, medidas y modelos de cláusulas/contratos utilizados:

  - con proveedores externos cuando éstos tengan acceso a datos personales de **MUGARIK GABE ONGD** para prestar el servicio, es decir cuando el proveedor sea un encargado de tratamiento. Mención especial a la transferencia internacional de datos.
  - cuando **MUGARIK GABE ONGD** tenga acceso a datos personales de clientes para prestar el servicio, es decir cuando **MUGARIK GABE ONGD** sea un encargado de tratamiento.
  - con proveedores que no tiene acceso a datos personales en función del servicio contratado, es decir no son encargados de tratamiento, pero si tiene acceso a instalaciones físicas dónde se presta el tratamiento y, por tanto, tiene que garantizar la confidencialidad de la información sobre datos personales.

- **Anexo 3_ Registro de Actividades de Tratamiento (RAT)**: cumple con la obligación de incluir la información exigida para cada uno de los tratamientos realizados, en calidad de

responsable o de encargado de tratamiento y además se incluyen aspectos relacionados con los sistemas de información de la Organización.

- **Anexo 4_ Medidas de Seguridad,** que contiene las Medidas de Seguridad de índole técnica y organizativa que es necesario adoptar, regulando de manera particular:

  - **Incidencias y Brechas de seguridad**, recoge el registro de incidencias que afectan o puedan afectar a la seguridad de los datos personales y las cuestiones relativas a la notificación ante la Agencia de Protección de datos y usuarios si procede.
  - **Control periódico,** contiene un documento de control para proceder a las revisiones y actualizaciones que se lleven a cabo periódicamente de este documento de seguridad y sus correspondientes anexos para dar cumplimiento a lo dispuesto en el art 24.1 del RGPD

2. POLÍTICA DE SEGURIDAD

MUGARIK GABE ONGD, en calidad de responsable de Tratamiento, es consciente de la importancia que tiene la normativa sobre Protección de Datos de Carácter Personal. Por ello desarrolla la siguiente Política, así como los correspondientes procedimientos e instrucciones organizativos y técnicos, de manera que se garantice la confidencialidad, integridad y disponibilidad de la información de una forma proporcional a los niveles de riesgo de la organización.

En base a esta política se definen los procedimientos más adecuados para la mejora de los procesos que tratan datos de carácter personal; por ello, cuando se detallen aplicaciones o soluciones concretas, se hará bajo dicha perspectiva, potenciando aquellas soluciones que lleven seguridad a la información relevante de **MUGARIK GABE ONGD**.

La intención final de todo el sistema definido y desarrollado en la documentación que se presenta, es la de ofrecer el mejor servicio a los titulares de datos de carácter personal respetando escrupulosamente la normativa y, especialmente, el ejercicio de los derechos legalmente establecidos.

Por todo ello, **MUGARIK GABE ONGD** quiere dejar constancia expresa de su conocimiento y de la aprobación de los procedimientos desarrollados en este documento, de forma que todo el personal los debe conocer y asumir como parte de sus funciones laborales.

Para que esto sea posible se asignarán los recursos necesarios, de manera proporcional, para el buen desarrollo de lo aquí establecido, tanto en el inicio de la adaptación a la normativa como en su mantenimiento futuro.

Todo el documento de seguridad, sus anexos y esta política se apoyan y sirven de base a la responsabilidad proactiva que **MUGARIK GABE ONGD** debe cumplir y demostrar.

3. RESPONSABILIDAD PROACTIVA

La responsabilidad proactiva es una de las directrices básicas establecidas en el artículo 5 del RGPD para el responsable del tratamiento de datos de carácter personal. En síntesis, la responsabilidad proactiva incluye los siguientes principios:

- Licitud, lealtad y transparencia en el tratamiento de datos personales del interesado.
- Limitación de la finalidad: los datos serán recogidos con fines determinados, explícitos y legítimos y no serán tratados con otra finalidad, salvo si es necesario, con fines de archivo de interés público, fines de investigación científica e histórica o fines estadísticos.
- Minimización de datos: los datos serán adecuados, pertinentes y limitados a lo necesario en relación a los fines para los que van a ser tratados.
- Exactitud: los datos serán exactos y actualizados, adoptándose medidas razonables para que se supriman o rectifiquen los datos que sean inexactos.
- Limitación del plazo de conservación: los datos serán mantenidos de forma que se permita la identificación de los afectados no más tiempo del necesario para los fines del tratamiento. Podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo de interés público, con fines de investigación científica e histórica o fines estadísticos, sin perjuicio de la aplicación de las correspondientes medidas técnicas y organizativas apropiadas que impone el RGPD.
- Integridad, confidencialidad y seguridad de los datos: serán tratados de manera que se garantice la adecuada seguridad, incluyendo la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, aplicando las medidas técnicas y de organización apropiadas.

Sobre la base anterior el responsable de tratamiento, es decir, **MUGARIK GABE ONGD**, para poder demostrar el cumplimiento de esta directriz debe tener la capacidad de proporcionar evidencias del cumplimiento de los distintos principios incluidos en la misma.

El RGPD establece un catálogo de medidas que el responsable y, en ocasiones los encargados, deben aplicar para garantizar que los tratamientos sean conformes al Reglamento. En el anexo correspondiente, se desglosan un catálogo de las mismas que inciden en el mencionado principio de responsabilidad proactiva, y que **MUGARIK GABE ONGD** tiene en cuenta como "hoja de ruta" para adaptar los datos personales que trata al RGPD.

4. TRANSPARENCIA DE INFORMACIÓN EN LA RECOGIDA DE DATOS PERSONALES

En aras de la transparencia en el tratamiento de los datos personales, el RGPD amplía considerablemente la información a los titulares de los datos en el momento de la recogida; entre otros, se deberá informar sobre los siguientes extremos:

- La base jurídica o legitimación del tratamiento;
- El plazo o criterios de conservación de la información;
- La existencia de decisiones automatizadas o elaboración de perfiles;
- La previsión de transferencias de datos a terceros países;
- En el caso de que los datos no se obtengan del propio afectado:
    - El origen de los datos;

  - Las categorías de los datos;
- Los derechos que asisten al titular de los datos personales., incluido el derecho a presentar una reclamación ante las autoridades de control.

En el caso de que los datos no se obtengan del propio afectado, por proceder de alguna cesión legítima, el responsable informará a las personas interesadas dentro de un plazo razonable de la obtención de los datos y en cualquier caso:

- Antes de un mes desde que se obtuvieron los datos personales;
- Antes o en la primera comunicación con el afectado;
- Antes de que los datos, en su caso, se hayan comunicado a otros destinatarios.

Los procedimientos de recogida de información pueden ser muy variados y, por tanto, los modos de informar a los afectados deben adaptarse a las circunstancias de cada uno de los medios empleados para la recopilación o registro de los datos.

En el caso de esta organización los modelos utilizados para cumplir esta obligación se incluyen en el **Anexo 1.**

5. DERECHOS DE LOS TITULARES DE LOS DATOS

Los derechos que los titulares puede ejercer conforme a RGPD son:

- **Derecho de acceso**: Conocer que datos dispone **MUGARIK GABE ONGD**, posibles comunicaciones y destinatarios, plazos de conservación.
- **Derecho de rectificación**: Rectificar los datos inexactos y/o incompletos.
- **Derecho de supresión** ("Derecho al olvido"): La supresión de los datos personales sin dilación debida.
- **Derecho a la limitación del tratamiento:** Solicitar al responsable la suspensión del tratamiento de datos o la conservación de los mismos para el ejercicio de otros derechos relacionados.
- **Derecho de portabilidad:** Solicitar la portabilidad de los datos tratados a un nuevo proveedor.
- **Derecho de oposición:** Oponerse al tratamiento de los datos.

Previa presentación de su documento nacional de identidad o pasaporte, los titulares de los datos personales podrán ejercer estos derechos. **MUGARIK GABE ONGD** dará respuesta a los interesados sin dilación indebida en el plazo de un mes. El desarrollo de este apartado se encuentra debidamente detallado en el **Anexo 1.**

6. BASES DE LEGITIMACIÓN DE LOS DATOS PERSONALES

El RGPD en su artículo 6 diseña un sistema de legitimación basado en seis bases jurídicas, que no mantienen entre sí ninguna relación de prioridad o prelación, y que son:

- consentimiento del interesado para el tratamiento de sus datos personales para uno o varios fines específicos;
- necesidad del tratamiento para:

  - la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;
  - el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
  - proteger intereses vitales del interesado o de otra persona física;
  - para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;
  - para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero.

El responsable de tratamiento deberá justificar los tratamientos de datos en una o varias de estas bases jurídicas. En caso de existir un cambio de base jurídica que justifique el tratamiento, los afectados deben ser informados y deben poder ejercer los derechos asociados a la nueva base.

En los casos en que la base jurídica de los tratamientos sea el **consentimiento**, éste deberá ser informado, libre, específico y otorgado por los afectados mediante una manifestación que muestre su voluntad de consentir o mediante una clara acción afirmativa.

Además, el consentimiento en el marco del RGPD se caracteriza por lo siguiente:

- Puede ser para uno o varios fines.
- Revocable.
- El responsable debe poder probar que ha obtenido el consentimiento.
- Utilizar un lenguaje claro y sencillo.

Las bases jurídicas de legitimación utilizadas por **MUGARIK GABE ONGD** para cada tratamiento se recogen y detallan en el Registro de Actividades de Tratamiento (RAT) desarrollado más adelante en este documento.

7. RELACIONES RESPONSABLE Y ENCARGADO

En materia de protección de datos, hay que distinguir cuando una organización actúa como:

- «**responsable del tratamiento**» o «responsable»: que es cuando, sola o junto con otros, determine los fines y medios del tratamiento, o
- «**encargado del tratamiento**» o «encargado»: es decir trata datos personales por cuenta del responsable del tratamiento.

El Considerando 81 del RGPD prevé que el encargado del tratamiento, debe ofrecer suficientes garantías en lo referente a conocimientos especializados, fiabilidad y recursos, con vistas a la aplicación de medidas técnicas y organizativas que cumplan los requisitos del RGPD, incluida la seguridad del tratamiento, así como del cumplimiento de la normativa de protección de datos,

por tanto **MUGARIK GABE ONGD** en calidad de responsable de tratamiento debe elegir como encargados del tratamiento a quien ofrezca garantías suficientes respecto a la implantación y el mantenimiento de las medidas técnicas y organizativas apropiadas, de acuerdo con lo establecido en el RGPD, y que garantice la protección de los derechos de las personas afectadas. Existe, por tanto, un deber de diligencia en la elección del responsable.

La regulación de la relación entre el responsable y encargado del tratamiento tiene que plasmarse en un contrato o acto jurídico similar por escrito que los vincule.

En el **Anexo 2** existe un modelo denominado Contrato del Proveedor- Encargado de Tratamiento para el caso que el Encargado de tratamiento no disponga de modelo apropiado.

Además de lo anterior, puede existir casos en los que **MUGARIK GABE ONGD** sea una encargada de tratamiento de datos personales, generalmente de un cliente u otra organización colaboradora, y ésta debe formalizar un contrato o acto de encargo de tratamiento con el mismo contenido descrito anteriormente, en el **Anexo 2** existe un modelo denominado Contrato de la Organización como Encargada de Tratamiento para el caso.

TRANSFERENCIA INTERNACIONAL DE DATOS

Las transferencias internacionales de datos suponen un flujo de datos personales desde el territorio español a destinatarios establecidos en países fuera del Espacio Económico Europeo (los países de la Unión Europea más Liechtenstein, Islandia y Noruega).

Los responsables y encargados del tratamiento podrán realizar transferencias internacionales de datos sin necesidad de una autorización de la Agencia Española de Protección de Datos siempre que el tratamiento de datos observe lo dispuesto en el RGPD, requisitos y procedimientos que se detallan en el **Anexo 2**.

PROVEEDORES Y COLABORADORES SIN ACCESO A DATOS

Para finalizar y dentro de este apartado, es necesario mencionar la figura del proveedor que no es encargado de tratamiento, pero si tiene acceso a instalaciones físicas dónde se presta el tratamiento de datos, y por tanto **MUGARIK GABE ONGD** tiene que garantizar la confidencialidad de la información sobre datos personales y para ello firma un acuerdo de confidencialidad, cuyo modelo, se incluye bajo la denominación “Contrato de Personal sin acceso a datos” en el **Anexo 2**, para el caso que el proveedor no tenga modelo específico al efecto.

8. REGISTRO DE ACTIVIDADES DE TRATAMIENTO

Hay que tener en cuenta que **MUGARIK GABE ONGD** en el desarrollo de sus actividades, puede manejar alguno de los siguientes datos personales:

- **Datos identificativos** (nombre y apellidos, NIF/DNI, nº Seguridad Social/Mutualidad, dirección, teléfono, firma, huella, imagen/voz, firma).

- **Datos identificativos** (nombre y apellidos, NIF/DNI, nº Seguridad Social/Mutualidad, dirección, teléfono, firma, huella, imagen/voz, firma).
- **Datos de características personales** (estado civil, datos de familia, fecha de nacimiento, lugar de nacimiento, edad, sexo, nacionalidad, lengua materna).
- **Datos de circunstancias sociales** (características de alojamiento/vivienda, aficiones y estilo de vida, pertenencia a clubes o asociaciones, licencias, permisos o autorizaciones).
- **Datos académicos y profesionales** (formación/titulaciones, historial académico, experiencia profesional, pertenencia a colegios o asociaciones profesionales).
- **Datos de detalles de empleo** (profesión, puesto de trabajo, historial del trabajador).
- **Datos económicos, financieros** (datos bancarios, datos económicos de nómina).
- **Datos de servicios:** Grabaciones de llamadas de clientes.

En ese sentido y según el artículo 30 del RGPD cada responsable y, en su caso, su representante deberá llevar un registro de las actividades de tratamiento (en adelante RAT) efectuadas bajo su responsabilidad.

El RAT se estructura en base a los siguientes puntos:

- Base de legitimación,
- Finalidad del tratamiento,
- Categoría de datos personales que trata,
- Categoría de titulares a los que pertenecen dichos tratamientos,
- Comunicación de estos datos a terceros: bien sea por cesión, por un encargado de tratamiento, o transferencia internacional de datos,
- Plazos durante los cuales se conservan los datos,
- Sistemas de Información que tratan los datos
- Medidas de seguridad a adoptar.

En el **Anexo 3** se desarrolla íntegramente el RAT de **MUGARIK GABE ONGD**.

9. ANÁLISIS DE RIESGOS

La norma europea introduce el análisis de riesgo para que en base al mismo poder establecer las medidas técnicas y organizativas necesarias para ofrecer un nivel de seguridad adecuado.

A través de este análisis de riesgo, se determinarán las medidas a aplicar para que los tratamientos de datos sean respetuosos con lo dispuesto en el RGPD.

10. MEDIDAS DE SEGURIDAD

La protección de los derechos y libertades de los ciudadanos en relación con el tratamiento de sus datos personales exige la adopción de medidas técnicas y organizativas con la finalidad de garantizar el cumplimiento de lo dispuesto en el RGPD.

A tenor del tipo de tratamientos expuestos en el RAT de **MUGARIK GABE ONGD** y al análisis de riesgo desarrollado para dichos tratamientos se definirán las medidas de seguridad técnicas, administrativas y organizativas a implementar en **MUGARIK GABE ONGD** y que se encuentran recogidas en **Anexo 4.**

11. QUIEBRAS DE SEGURIDAD DE LOS DATOS PERSONALES

Cuando se produzca una violación o quiebra de seguridad, es decir, cuando se produzca la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizado a dichos datos, siempre que exista riesgo para los derechos y libertades de las personas físicas, **MUGARIK GABE ONGD** deberá notificarlo la AEPD, en un plazo máximo de 72 horas.

La notificación se realizará por medios electrónicos a través de la sede electrónica de la Agencia Española de Protección de Datos en la dirección: https://sedeagpd.gob.es

Deberá avisarse también a las personas físicas cuyos datos personales se hayan visto afectados por la quiebra de seguridad cuanto antes.

Existen EXCEPCIONES a la obligación de realizar estas comunicaciones, que son:

- Si se han adoptado y aplicado medidas sobre los datos personales afectados, particularmente aquellas que hagan ininteligibles los datos para cualquier persona que no esté autorizada a acceder ellos (p.e.: cifrado de datos personales).
- El responsable ha adoptado medidas ulteriores que garanticen que ya no existe un alto riesgo para los derechos y libertades.
- Que la comunicación suponga un esfuerzo desproporcionado, optándose por una comunicación pública o medida semejante por la que se informe de forma efectiva a los afectados.

12. REVISIÓN PERIÓDICA DE LAS MEDIDAS DE SEGURIDAD

MUGARIK GABE ONGD en cumplimiento del RGPD aplica medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Además, el propio Reglamento establece la obligación de que dichas medidas se revisen y actualicen cuando sea necesario. Por lo tanto, es necesario realizar controles periódicos sobre la adecuación de las medidas, identificación de deficiencias y propuesta de las medidas correctoras o complementarias necesarias.

Así se recoge en el **Anexo 4. Control Periódico** el procedimiento correspondiente con el objeto de llevar una revisión periódica de la adecuación del documento de seguridad de **MUGARIK GABE ONGD** y sus anexos a la normativa vigente en la materia.