DOCUMENTACIÓN DE PROTECCIÓN DE DATOS

Adecuación al Reglamento General de Protección de Datos y a la LOPD

ISABEL BUEZO Y JOSE ANTONIO GOMEZ SAINZ DE LA MAZA CB

ÚLTIMA ACTUALIZACIÓN: 10 DE MAYO DE 2021

ÍNDICE

INTRODUCCIÓN

El objetivo del presente documento es llevar a cabo la implantación efectiva de la nueva normativa de protección de datos -principalmente, del 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- a partir de ahora, RGPD) y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (a partir de ahora, LOPDGDD)- en la entidad ISABEL BUEZO Y JOSE ANTONIO GOMEZ DE LA MAZA CB. Asimismo, tiene por objeto informar y formar a todas las personas que manejan datos en dicha organización para que el tratamiento de datos cumpla de forma real con los postulados de la normativa sobre protección de datos de carácter personal.

En todo caso, el presente documento deberá ser actualizado en todo momento, siendo revisado siempre que haya cambios, tanto en el sistema de información o en la organización del mismo como en las categorías de datos o el tratamiento de los mismos. De igual modo, deberá ser modificado ante cualquier cambio legislativo, para adaptarlo a las disposiciones vigentes en materia de seguridad y protección de datos de carácter personal. De esta forma, el documento intentará ser un marco estable y, al mismo tiempo, flexible, en lugar de una descripción estática, por lo que estará sometido a continuas actualizaciones.

ÁMBITO DE APLICACIÓN DEL DOCUMENTO

Los recursos comprendidos dentro del ámbito de aplicación de este documento serán todos los datos de carácter personal que conforman el Registro de Actividades de Tratamiento de ISABEL BUEZO Y JOSE ANTONIO GOMEZ DE LA MAZA CB, así como todas las aplicaciones y sistemas que los traten, los equipos informáticos que los soportan y los locales (físicos o virtuales) donde se ubiquen. El detalle de los diferentes tratamientos se describe en el mencionado Registro de Actividades de Tratamiento, que deberá mantenerse actualizado en todo momento y que quedará elaborado en conformidad con el artículo 30 del RGPD y con el artículo 31 de la LOPDGDD.

Para dar cumplimiento al principio de responsabilidad proactiva o *accountability*, que hace referencia a la prevención por parte de las organizaciones que tratan datos personales, se deberán

aplicar las medidas de seguridad necesarias para garantizar los criterios de seguridad correspondientes: confidencialidad, integridad, disponibilidad y resiliencia.

Finalmente, el responsable del tratamiento será quien deba asegurarse del cumplimiento de tales medidas de seguridad que se detallan en el presente Documento de Seguridad.

INFORME DELEGADO DE PROTECCIÓN DE DATOS (DPD)

1. Objetivos

El nuevo Reglamento (UE) General de Protección de Datos -en los artículos 37 a 39- introduce una nueva figura, desconocida para la legislación precedente; figura que es desarrollada en los artículos 34 a 37 de la LOPDGDD. Es el denominado Delegado de Protección de Datos (en adelante, DPD), cuyo nombramiento no es obligatorio para todas las empresas, aunque siempre se puede asumir voluntariamente (artículo 34.2 LOPDGDD). El objetivo de este Informe es analizar, a la luz de la legislación existente a día de hoy, así como de las Resoluciones, Directrices, Recomendaciones… de las Autoridades de Control, con especial referencia a la Agencia Española de Protección de Datos y al Grupo de Trabajo de Protección de Datos del Artículo 29, para intentar llegar a una conclusión satisfactoria sobre la necesidad de nombramiento o no de Delegado de Protección de Datos por parte de la entidad anteriormente descrita, teniendo en cuenta las dificultades que plantea el nuevo Reglamento General de Protección de Datos y la nueva LOPDGDD.

Asimismo, se hará referencia, a lo largo del Informe, el señalar la posición que debe ocupar el Delegado de Protección de Datos, así como los requisitos y funciones que debe desempeñar esta figura novedosa, su régimen de responsabilidad y garantías y otras consideraciones de interés, las cuales habrá que tener en cuenta a la hora de decidirse a nombrar un Delegado de Protección de Datos, ya sea en el interior de la propia organización o como figura externa, así como en el caso de ser obligatoria su designación o si voluntariamente se quisiera asumir.

2. Obligatoriedad de nombramiento de DPD

Los artículos 37 a 39 del Reglamento General de Protección de Datos (RGPD) señalan que será obligatorio el nombramiento de DPD en:

- Administraciones y organismos públicos.

- Responsables o Encargados que tengan entre sus actividades principales las operaciones de tratamiento que requieran una observación habitual y sistemática de interesados a gran escala.
- Responsables o Encargados que tengan entre sus actividades principales el tratamiento a gran escala de datos sensibles.

Hay que tener en cuenta que, con arreglo al artículo 37 apartado 4 del RGPD, el Derecho de la Unión o de los Estados miembro podrá exigir el nombramiento de un DPD también en otras situaciones. Teniendo en cuenta esto, en España también será de aplicación la citada Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD), en cuyo artículo 34 se dice que, además, deberán nombrar un DPD:

a) Los colegios profesionales y sus consejos generales.
b) Los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas.
c) Las entidades que exploten redes y presten servicios de comunicaciones electrónicas conforme a lo dispuesto en su legislación específica, cuando traten habitual y sistemáticamente datos personales a gran escala.
d) Los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio.
e) Las entidades incluidas en el artículo 1 de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito.
f) Los establecimientos financieros de crédito.
g) Las entidades aseguradoras y reaseguradoras.
h) Las empresas de servicios de inversión, reguladas por la legislación del Mercado de Valores.
i) Los distribuidores y comercializadores de energía eléctrica y los distribuidores y comercializadores de gas natural.
j) Las entidades responsables de datos comunes para la evaluación de la solvencia patrimonial y crédito o de los datos comunes para la gestión y prevención del fraude, incluyendo a los responsables de los datos regulados por la legislación de prevención del blanqueo de capitales y de la financiación del terrorismo.

k) Las entidades que desarrollen actividades de publicidad y prospección comercial, incluyendo las de investigación comercial y de mercados, cuando lleven a cabo tratamientos basados en las preferencias de los afectados o realicen actividades que impliquen la elaboración de perfiles de los mismos.

l) Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes. Se exceptúan los profesionales de la salud que, aun estando legalmente obligados al mantenimiento de las historias clínicas de los pacientes, ejerzan su actividad a título individual.

m) Las entidades que tengan como uno de sus objetos la emisión de informes comerciales que puedan referirse a personas físicas.

n) Los operadores que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos, conforme a la normativa de regulación del juego.

o) Las empresas de seguridad privada.

p) Las federaciones deportivas cuando traten datos de menores de edad.

3. Posición del DPD

El DPD, en virtud de los artículos 35 y 36 de la LOPDGDD, deberá ser nombrado en atención a sus cualificaciones profesionales y, en particular, a su conocimiento sobre la legislación aplicable y la práctica de la protección de datos. Aunque no debe tener una titulación específica, los conocimientos jurídicos en la materia son, sin duda, necesarios, pero también es ineludible contar con conocimientos ajenos al ámbito estrictamente jurídico, tales como conocimientos en materia de tecnología aplicada al tratamiento de datos personales, así como conocimientos en relación al ámbito de actividad de la organización en la que desempeñe la tarea el DPD.

En cuanto al nivel de conocimientos exigido, no está definido estrictamente, pero debe ser acorde con la sensibilidad, complejidad y cantidad de los datos que una organización trata. Por ejemplo, cuando la actividad de tratamiento sea especialmente compleja o cuando implique una gran cantidad de datos sensibles, el DPD podría necesitar un mayor nivel de conocimientos y apoyo. También, habrá que tener en cuenta cuestiones tales como si la empresa transfiere datos fuera de la UE o si dichas transferencias son ocasionales.

En relación a las cualidades profesionales, el RGPD no las especifica con precisión, pero es importante que tenga conocimientos sobre la legislación y prácticas nacionales y europeas en materia de protección de datos y una profunda comprensión del RGPD y de la LOPDGDD. Asimismo, es útil el conocimiento acerca del sector de la propia organización y de las operaciones de tratamiento que se llevan a cabo en la misma, así como de los sistemas de información y de las necesidades de seguridad y protección de datos. Una vez se designe un DPD, sus datos de contacto tendrán que hacerse públicos por los responsables y encargados y deben ser comunicados a las autoridades de supervisión competentes, en este caso a la Agencia Española de Protección de Datos (AEPD).

4. Requisitos que debe cumplir la figura del DPD y funciones

Dentro de la organización, la posición del DPD tiene que cumplir unos requisitos, que son los siguientes (véase artículo 36 de la LOPDGDD):

- Autonomía e independencia totales en el ejercicio de sus funciones.
- Necesidad de que se relacione con el nivel superior de la dirección.
- Obligación de que el responsable o el encargado faciliten al DPD todos los recursos necesarios para desarrollar su actividad.

De este modo, el DPD se convierte en una figura estratégica entre la empresa, los clientes y la Autoridad de Control, de forma que las funciones se pueden dividir en tres categorías:

- *Función interna* (propia organización). Será el encargado de coordinar todos los procedimientos que se refieran al tratamiento de datos personales, de supervisar que la normativa sobre protección de datos se cumple, formación de empleados y demás personal de la empresa que trate datos de carácter personal…;
- *Función de cooperación con la Autoridad de Control*. Será el intermediario entre la empresa y la AEPD, quien deba relacionarse y colaborar con las Autoridades de Control en caso de denuncia, inspección, comunicación de brecha de seguridad…:
- *Función mediadora con ciudadanos*. Será el punto de contacto con los ciudadanos, de forma que le corresponderá atender las peticiones de clientes, ejercicio de sus derechos o acercar posiciones entre las partes (ciudadanos y la organización) y proponer un acuerdo o reparación para evitar que el conflicto llegue a la AEPD.

El DPD, en definitiva, debe ser aquella persona que promocione la cultura de protección de datos en el seno de la propia organización y contribuya a la aplicación de elementos esenciales del RGPD, como los principios relativos al tratamiento de datos, los derechos de los interesados, la protección de datos desde el diseño y por defecto, el Registro de las Actividades de Tratamiento, la seguridad del tratamiento y la notificación y comunicación de las violaciones de seguridad de los datos.

5. Publicación y comunicación de los datos de contacto del DPD

El apartado 7 del artículo 37 del RGPD requiere que el responsable y/o encargado del tratamiento:

- Publiquen los datos de contacto del DPD y;
- Comuniquen los datos de contacto del DPD a las correspondientes autoridades de control.

Los datos de contacto del DPD deben incluir información que permita a los interesados y a las autoridades de control comunicarse con este de forma sencilla (número de teléfono específico y/o una dirección de correo electrónico específica). Cuando corresponda, a efectos de comunicación con el público, podrían facilitarse otros medios de comunicación, por ejemplo, una línea directa específica o un formulario de contacto específico dirigido al DPD en el sitio web de la organización). Se recomienda, también, que las organizaciones informen a sus empleados del nombre y datos de contacto del DPD. El canal para la publicación y comunicación de los datos de contacto del DPD es el siguiente:

https://sedeagpd.gob.es/sede-electronica-web/vistas/formDelegadoProteccionDatos/procedimientoDelegadoProteccion.jsf.

6. Responsabilidad del DPD

Los DPD no son personalmente responsables en caso de incumplimiento del RGPD, puesto que es el responsable y/o el encargado los que están obligado a garantizar y ser capaces de demostrar que el tratamiento se realiza de conformidad con el RGPD (artículo

24.1). Por consiguiente, el cumplimiento de las normas sobre protección de datos es responsabilidad del responsable y/o del encargado del tratamiento.

Esto implica que el responsable del tratamiento no solo responde ante posibles sanciones que se impongan al Delegado de Protección de Datos, sino que también deberá ser responsable ante indemnizaciones que sean exigidas por el interesado a consecuencia de daños y perjuicios sufridos al haberse producido una infracción del RGPD. Es más, el artículo 70.2 de la LOPDGDD establece la no responsabilidad del Delegado de Protección de Datos, en el sentido de que "no será de aplicación al delegado de protección de datos el régimen sancionador establecido en este Título".

Por ello, el Delegado de Protección de Datos que haya sido designado por la empresa y siempre que se limite a la función por la que ha sido designado y conforme a la normativa pertinente, así como al buen cumplimiento en las labores correspondientes, no se le podrá exigir responsabilidad que establezca la normativa en protección de datos. Para ello, el Delegado de Protección de Datos no podrá ser destituido ni sancionado por la empresa si en el ejercicio de sus funciones ha actuado conforme a lo establecido en la normativa.

7. Recursos que el responsable o encargado de tratamiento debe asignar al DPD

El DPD debe contar con los recursos necesarios para el desempeño de sus funciones. Dependiendo de la naturaleza de las actividades de tratamiento y de la actividad y el tamaño de la organización, se deberán asignar los siguientes recursos al DPD:

- Apoyo activo al DPD por parte de la dirección;
- Tiempo suficiente para que el DPD cumpla con sus funciones;
- Apoyo adecuado en cuanto a recursos financieros, infraestructura (equipos, instalaciones) y personal según se requiera;
- Comunicación oficial de la designación de DPD a toda la plantilla;
- Acceso a otros servicios dentro de la organización de modo que los DPD puedan recibir apoyo esencial, datos e información de dichos servicios;
- Formación continua.

8. Garantías que permiten al DPD desempeñar su función de manera independiente

Diversas salvaguardias permiten al DPD desempeñar sus funciones de manera independiente (artículo 36 LOPDGDD):

- El DPD no recibirá instrucciones por parte del responsable o encargado del tratamiento en lo relativo al ejercicio de sus funciones como DPD;
- No podrá ser sancionado o destituido por el responsable del tratamiento por el desempeño de sus funciones;
- No habrá conflictos de intereses con otras posibles funciones y obligaciones.

Las otras funciones y obligaciones de un DPD que desarrolle en la organización no deben llevar a un conflicto de intereses. Esto significa que el DPD no puede ocupar un cargo en la empresa que le lleve a determinar los fines y medios del tratamiento de datos personales. Los cargos en conflicto, como norma general, dentro de una organización pueden incluir los puestos de alta dirección, pero también otros cargos inferiores si tales cargos o puestos llevan a la determinación de los fines y medios del tratamiento.

9. Consideraciones previas a tener en cuenta

- Se permite nombrar un solo DPD para un grupo empresarial, siempre que sea accesible desde cada establecimiento del grupo.
- La AEPD ha optado por promover un sistema de certificación de profesionales de protección de datos, como herramienta para evaluar que los candidatos a ocupar el puesto de DPD reúnen las cualificaciones profesionales y los conocimientos requeridos. Dichas certificaciones serán otorgadas por entidades certificadoras debidamente acreditadas por la Entidad Nacional de Acreditación, siguiendo criterios de acreditación y certificación elaborados por la AEPD en colaboración con los sectores afectados.
- La certificación, en principio y a día de hoy, no será un requisito indispensable para el acceso a la profesión, sino que será solo una opción a disposición de responsables y encargados para facilitar su selección de los profesionales que estén llamados a ocupar el puesto de DPD. Pero, responsables y encargados pueden tomar en consideración otras cuestiones u otros medios para demostrar la competencia de los DPD.

- Se permite que el DPD mantenga con responsables o encargados una relación laboral o mediante un contrato de servicios. Es decir, permite que pueda contratarse el servicio de DPD con personas físicas o jurídicas ajenas a la organización.
- Se permite que el DPD desarrolle sus funciones a tiempo completo o parcial. En este último caso, es preciso evitar que existan conflictos de intereses. Estos conflictos pueden surgir cuando el DPD, en su tarea de supervisión de las actividades de tratamiento de datos llevadas a cabo por la organización, deba valorar su propio trabajo dentro de ella, como sucede si se designa DPD al responsable de tecnologías de la información (cuando estas tecnologías se emplean para el tratamiento de datos) o al responsable de un área de negocio que decide sobre determinados tratamientos.

10. Consideraciones sobre la obligatoriedad de nombrar DPD

El RGPD, en relación a aquellos casos que es necesario nombrar DPD, como se ha visto, reviste cierta ambigüedad, puesto que existen "zonas oscuras" que no permiten vislumbrar con claridad si existe obligación o no de nombramiento de DPD. Para intentar esclarecer, en lo que a este caso se refiere y si sería necesario dicho nombramiento, es muy conveniente tener en cuenta las "Directrices sobre los delegados de protección de datos (DPD)", elaboradas por el Grupo de Trabajo del Artículo 29 (en adelante, GT29) el 13 de diciembre de 2016 y revisadas por última vez y adoptadas el 5 de abril de 2017, donde se establecen determinadas pautas en relación a esta figura.

Dichas "zonas oscuras" que se contienen en el artículo 37 RGPD principalmente son las referidas a "autoridad u organismo público", "actividades principales", "a gran escala", "observación habitual y sistemática" y "categorías especiales de datos y datos relativos a condenas e infracciones". En lo que a este caso interesa, es necesario hacer mención a las siguientes:

- *"Actividades principales"*. El artículo 37, apartado 1, letras b) y c) del RGPD se refiere a las "actividades principales del responsable o del encargado". El considerando 97 especifica que las actividades principales pueden considerarse las operaciones clave necesarias para lograr los objetivos del responsable o del encargado de tratamiento. Según el GT29, "las actividades principales no deben interpretarse como excluyentes cuando el tratamiento de datos sea una parte indisociable de la actividad del responsable

o encargado del tratamiento. Por ejemplo, la actividad principal de un hospital es prestar atención sanitaria. Sin embargo, un hospital no podría prestar atención sanitaria de manera segura y eficaz sin tratar datos relativos a la salud, como las historias clínicas de los pacientes. Por tanto, el tratamiento de dichos datos debe considerarse una de las actividades principales de cualquier hospital, y los hospitales deben, en consecuencia, designar un DPD".

- *"A gran escala"*. El artículo 37, apartado 1, letras b) y c), establece que el tratamiento de datos personales debe realizarse a gran escala para que sea obligatorio la designación de un DPD. El RGPD no define qué se debe entender "a gran escala", pero se puede acudir al Considerando 97, el cual puede ofrecer orientaciones. Sin embargo, no es posible, a día de hoy, ofrecer una cifra exacta, ya sea con relación a la cantidad de datos procesados o al número de personas afectadas, que pudiera aplicarse a todas las situaciones. En cualquier caso, el GT29 recomienda que se tengan en cuenta los siguientes factores a la hora de determinar si un tratamiento de datos se realiza a gran escala:
  - El número de interesados afectados, bien como cifra concreta o como proporción de la población correspondiente;
  - El volumen de datos o la variedad de elementos de datos que son objeto de tratamiento;
  - La duración, o permanencia, de la actividad de tratamiento de datos;
  - El alcance geográfico de la actividad de tratamiento.

- *"Observación habitual y sistemática"*. La noción de observación habitual y sistemática de interesados no está definida en el RGPD, pero el concepto de «observación del comportamiento de los interesados» se menciona en el considerando 24 e incluye claramente toda forma de seguimiento y creación de perfiles en internet, también con fines de publicidad comportamental. No obstante, el concepto de observación no se limita al entorno en línea y el seguimiento en línea debe considerarse solo un ejemplo de observación del comportamiento de los interesados. El Grupo de Trabajo del artículo 29 interpreta «habitual» con uno o más de los siguientes significados:
  - continuado o que se produce a intervalos concretos durante un periodo concreto;
  - recurrente o repetido en momentos prefijados;

- que tiene lugar de manera constante o periódica.

El Grupo de Trabajo interpreta «sistemático» con uno o más de los siguientes significados:

- que se produce de acuerdo con un sistema;
- preestablecido, organizado o metódico;
- que tiene lugar como parte de un plan general de recogida de datos;
- llevado a cabo como parte de una estrategia.

Ejemplos de actividades que pueden constituir una observación habitual y sistemática de interesados son: operar una red de telecomunicaciones; prestar servicios de telecomunicaciones; redireccionar correos electrónicos; actividades de mercadotecnia basadas en datos; elaborar de perfiles y otorgar puntuación con fines de evaluación de riesgos (p. ej. para determinar la calificación crediticia, establecer primas de seguros, prevenir el fraude, detectar blanqueo de dinero); llevar a cabo un seguimiento de la ubicación, por ejemplo, mediante aplicaciones móviles; programas de fidelidad; publicidad comportamental; seguimiento de los datos de bienestar, estado físico y salud mediante dispositivos ponibles; televisión de circuito cerrado; dispositivos conectados, como contadores inteligentes, coches inteligentes, domótica, etc.

11. Conclusiones

Con todo ello, DEBEMOS ENTENDER QUE NO EXISTE OBLIGATORIDAD EN EL NOMBRAMIENTO DE DELEGADO DE PROTECCIÓN DE DATOS, en virtud del artículo 37 del RGPD y de las Directrices elaboradas por el Grupo de Trabajo del Artículo 29.

No obstante, las ventajas de nombrar un DPD (ya sea obligatorio o voluntario) merecen una reflexión. Facilitar el cumplimiento de la normativa de protección de datos, cumplir con el principio de *accountability* y proactividad, así como disponer de una ventaja competitiva y de una imagen más profesional, pueden ser muy positivos para decantarse por el nombramiento de un DPD.

A menos que resulte obvio que a una empresa no se le requiere la designación de un DPD, el Grupo de Trabajo del Artículo 29 recomienda que los responsables y encargados del tratamiento documenten el análisis interno realizado para determinar si debe nombrarse o no un DPD. Este análisis forma parte de la información requerida con arreglo al principio de rendición de cuentas, que puede ser exigida por la autoridad de control y debe actualizarse cuando sea necesario (por ejemplo, si la organización se dedica a nuevas actividades o prestan servicios nuevos).

El DPD designado por un encargado del tratamiento también supervisará las actividades realizadas por la organización del encargado cuando actúe como responsable del tratamiento por derecho propio. Si la empresa no está obligada a nombrar DPD y voluntariamente no lo asume, nada impide que esa organización pueda emplear personal propio o asesores externos que desempeñen tareas relacionadas con la protección de datos personales. En tal caso, es importante asegurarse que no haya confusión con respecto al cargo, status, puesto y tareas. Por ello, debe quedar claro, en cualquier comunicación dentro de la empresa, así como con las autoridades de control, los interesados y el público en general, que el título de esta persona o asesor no es el de DPD.

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

a. Información Previa

Siguiendo con el apartado 1 del artículo 30 del 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 –a partir de ahora, RGPD), "cada responsable y, en su caso, su representante llevará un registro de las actividades de tratamiento efectuadas bajo su responsabilidad". Es más, "cada encargado y, en su caso, el representante del encargado, llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable". Esta tesis es respaldada por la LOPDGDD en su artículo 31.

En la práctica puede identificarse un tratamiento como el conjunto de operaciones dirigidas a conseguir una determinada finalidad que se legitiman en una misma base jurídica. Cada tratamiento incluirá una serie de operaciones como, por ejemplo, la recogida, registro, organización, estructuración, consulta o utilización de los datos. Por consiguiente, una

actividad de tratamiento se debe incluir en el registro de actividades en el momento previo antes de su puesta en marcha. Para facilitar la documentación del registro se puede utilizar la información previa documentada en los análisis iniciales realizados durante la fase de definición de la operación de tratamiento, sin olvidar que la estructura del mismo deberá corresponder a lo que el punto 1 del artículo 30 del RGPD y artículo 31 de la LOPDGDD detallan.

Así las cosas, la identificación y descripción de las actividades del tratamiento, no solo es una obligación, sino una necesidad en las fases iniciales para facilitar el análisis de riesgos; y es que cada responsable de tratamiento deberá valorar el grado de segregación o agregación al que somete sus tratamientos generando elementos diferentes que se corresponden con finalidades, bases jurídicas y grupos de individuos distintos.

Artículo 30 del RGPD

"El responsable o el encargado del tratamiento y, en su caso, el representante del responsable o del encargado pondrán el registro a disposición de la autoridad de control que lo solicite".

Por tanto, es fundamental que el registro de actividades esté permanentemente actualizado y en un formato claro y legible que facilite su comprensión por parte de terceros. El registro de actividades de tratamiento se debe entender, necesariamente, como un documento vivo, que requiere revisión continua y actualización cada vez que se produzca un cambio relevante en alguna actividad de tratamiento registrada. Por otra parte, dicho registro deberá contener toda la información indicada a continuación (vid. artículo 30 del RGPD):

- el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos;
- los fines del tratamiento;
- una descripción de las categorías de interesados y de las categorías de datos personales;
- las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;
- en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional

y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;

- cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;
- cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32, apartado 1.

b. Registro de Actividades de Tratamiento (en calidad de responsable del tratamiento)

ISABEL BUEZO Y JOSE ANTONIO GOMEZ DE LA MAZA CB actúa en calidad de responsable del tratamiento respecto de los datos de sus clientes, de potenciales clientes, y de sus proveedores.

DATOS DE IDENTIFICACIÓN

Responsable del tratamiento	ISABEL BUEZO Y JOSE ANTONIO GOMEZ DE LA MAZA CB
Número de identificación	J95720512
Dirección postal	GETXO, CALLE AMAIA 22 BJ
Teléfono de contacto	944315467
Correo electrónico	oicarseleccion@gmail.com
Actividad realizada	AGENCIA DE COLOCACION

CLIENTES Y POSIBLES CLIENTES

Finalidad del tratamiento	Gestión de la relación con los clientes
Base de legitimación para el tratamiento	Ejecución de un contrato (art. 6.1,b RGPD)

Descripción de la categoría de clientes	Personas con las que se mantiene una relación comercial como clientes
Descripción de las categorías de datos personales	Los necesarios para el mantenimiento de la relación comercial, prestar un servicio, facturar, enviar publicidad y servicio de postventa y fidelización: • De identificación: nombre y apellidos, NIF, dirección postal, teléfonos, e-mail. • Datos formativos y de experiencia laboral • Datos bancarios. • Datos de salud y relativos a las relaciones familiares • Características personales: edad, género y sexo
Origen y procedencia de los datos	Los propios interesados (o sus representantes legales)
Comunicación de datos a terceros	Cumplimiento, en su caso, de obligaciones legales: • Administración Tributaria • Seguridad Social • Cuerpos y Fuerzas de Seguridad del Estado. • Bancos y entidades financieras. • Interesados en los servicios que prestan los clientes
Duración del tratamiento/Conservación de los datos	Los previstos por la legislación fiscal respecto a la prescripción de responsabilidades
Medidas de seguridad	Las medidas de seguridad técnicas y organizativas implantadas se corresponden con las previstas en el artículo 32.1 del Reglamento (UE) General de Protección de Datos. Las medidas concretas quedan redactadas en el Documento de Seguridad.

PROVEEDORES (PERSONAS FÍSICAS)	
Finalidad del tratamiento	Gestión de la relación con los proveedores
Descripción de la categoría de proveedores	Personas con las que se mantiene una relación comercial como proveedores de productos y/o servicios
Descripción de las categorías de datos personales	Los necesarios para el mantenimiento de la relación contractual, facturación y realizar pedidos: • De identificación: nombre, NIF, dirección postal, teléfonos, e-mail. • Datos bancarios: para la domiciliación de pagos
Comunicación de datos a terceros	Cumplimiento, en su caso, de obligaciones legales: • Administración tributaria • Seguridad Social • Cuerpos y Fuerzas de Seguridad del Estado. • Bancos y entidades financieras. Otros: • Gestoría
Duración del tratamiento/Conservación de los datos	Los previstos por la legislación fiscal respecto a la prescripción de responsabilidades
Medidas de seguridad	Las medidas de seguridad técnicas y organizativas implantadas se corresponden con las previstas en el artículo 32.1 del Reglamento (UE) General de Protección de Datos. Las medidas concretas quedan redactadas en el Documento de Seguridad.

ANÁLISIS DE RIESGOS Y NECESIDAD DE EVALUACIÓN DE IMPACTO

1. Información General

El siguiente cuestionario pretende analizar si la iniciativa realizada por el área implica tratamiento de datos de carácter personal sujetos al marco jurídico que regula el derecho de protección de datos y valorar si en el tratamiento concurren circunstancias y situaciones que obliguen a realizar una Evaluación de Impacto en la Protección de Datos (EIPD). Dicho lo cual el análisis básico de riesgos es un análisis de mínimos que tiene como objetivo simplificar el proceso de análisis de riesgos en aquellas actividades de tratamiento con baja exposición al riesgo.

2. Información específica (en calidad de responsable del tratamiento)

ISABEL BUEZO IBAÑEZ Y JOSE ANTONIO GOMEZ SAINZ DE LA MAZA CB actúa en calidad de responsable del tratamiento respecto de los datos de sus clientes, de potenciales clientes y de sus proveedores.

DATOS DE IDENTIFICACIÓN

Responsable del tratamiento	ISABEL BUEZO IBAÑEZ Y JOSE ANTONIO GOMEZ SAINZ DE LA MAZA CB
Número de identificación	J95720512
Dirección postal	GETXO, CL AMAIA 22 BJ
Teléfono de contacto	944315467
Correo electrónico	oicarseleccion@gmail.com
Actividad realizada	AGENCIA DE COLOCACION

¿SE TRATAN DATOS PERSONALES DE PERSONAS FÍSICAS?	SI / NO
	SI

Finalidades del tratamiento	SI / NO
¿La recogida de los datos tiene como finalidad el tratamiento a gran escala?	NO
El número de sujetos afectados	0-10.000
Las categorías de datos tratados. (Datos especialmente protegidos, Datos de carácter identificativo, Características personales, Circunstancias sociales, Datos académicos y profesionales, Detalles del empleo, Información comercial, Datos económicos, financieros y de seguro, Transacciones de bienes y servicios).	Datos especialmente protegidos. Datos de carácter identificativo. Características personales. Datos académicos y profesionales. Detalles del empleo.
La duración del tratamiento (instantáneo (I), días (D), semanas (S), meses (M))	Por lo general, meses (M)
La extensión geográfica del tratamiento (Tratamiento a nivel regional (R), nacional (N) o internacional (I))	Por lo general, regional (R)
¿La recogida de los datos tiene como finalidad la monitorización o evaluación sistemática y exhaustiva de aspectos personales? (tratamiento para monitorizar, observar y/o controlar a los interesados, a través del cual, se pueden determinar hábitos, comportamientos, preferencias, gustos, intereses, etc. de personas identificadas o identificables)	NO.
¿La recogida de los datos tiene como finalidad exclusiva el tratamiento de datos especialmente protegidos?	NO.
¿El tratamiento involucra contacto con los interesados de manera que, dicho contacto, pueda resultar intrusivo? ¿Se prevé el uso de tecnologías que se pueden percibir como especialmente intrusivas en la privacidad?	NO. NO.
¿La finalidad del tratamiento implica el uso específico de datos de personas con discapacidad o cualquier otro colectivo en situación de especial vulnerabilidad (p.e.: menores de 14 años, ancianos, personas con riesgo de exclusión social, empleados, …)**?**	SI. ANCIANOS
¿Se van a tratar datos personales para elaborar perfiles, categorizar/segmentar, hacer ratings/scoring o para la toma de decisiones?	NO
¿El tratamiento de los datos implica una toma de decisiones automatizada sin que haya ninguna persona que intervenga en la decisión o valore los resultados?	NO
¿Se enriquece la información de los interesados mediante la recogida de nuevas categorías de datos? ¿Se usan las existentes con nuevas finalidades que antes no se contemplaban, en particular, si estas finalidades son más intrusivas o inesperadas para los afectados, o incluso pueda llegar a bloquear el disfrute de algún servicio?	NO. NO.
¿El tratamiento implica que un elevado número de personas (más allá de las necesarias para llevar a cabo el mismo) tenga acceso a los datos personales tratados?	NO

¿Se van a tratar datos relativos a la observación de zonas de acceso público?	NO
Para llevar a cabo este tratamiento, ¿se combinan conjuntos de datos utilizados por otros responsables de tratamiento cuya finalidad diste en exceso de las expectativas del interesado?	NO
¿Se utilizan datos de carácter personal no disociados o no anonimizados de forma irreversible con fines estadísticos, históricos o de investigación científica?	NO

Tecnologías empleadas para el tratamiento	SI / NO
¿Se prevé el uso de tecnologías que se pueden percibir como inmaduras, de reciente creación o salida al mercado, cuyo alcance no puede ser previsto por el interesado de forma clara o razonable e implique elevado riesgo para el acceso no autorizado?	NO

Cesiones de datos y Transferencias internacionales de datos	SI / NO
¿Se realizan cesiones de datos a otras entidades, ya sean del mismo grupo o proveedores externos al mismo?	SI
En caso afirmativo, ¿a quién?	• Gestoría • Posibles interesados en los servicios de los clientes.
En caso afirmativo, ¿para qué?	Mantenimiento y cumplimiento de la relación contractual y cumplimiento de obligaciones legales.
¿Se realizan transferencias internacionales de datos a países fuera de la Unión Europea y que no cuenten con medidas de protección de datos de carácter personal similares a las establecidas por la Autoridad de Control?	NO
En caso afirmativo, ¿cuáles?	

Percepción de la existencia de riesgo elevado	SI / NO
¿Es este tratamiento similar a otro para el que haya sido necesario realizar un EIPD?	NO
¿Este tratamiento puede conllevar una pérdida o alteración de la información?	NO
¿Se utilizada documentación en papel para tratar datos personales?	SI

En caso afirmativo, ¿qué medidas de protección se toman?	Se destruye de forma confidencial Puertas de entrada externas Se guardan bajo llave (caja fuerte)

Terceros que intervengan en el tratamiento	SI / NO
¿Interviene algún proveedor en el proceso?	SI
En caso afirmativo, ¿cuáles?	• Gestoría • Aplicaciones de gestión interna
En caso afirmativo, ¿por qué?	Mantenimiento y cumplimiento de la relación contractual y cumplimiento de obligaciones legales

Gestión de riesgos por defecto	SI / NO
¿Se prevén medidas para garantizar la protección de la información?	SI
En caso afirmativo, ¿cuáles?	Se destruye de forma confidencial Puertas de entrada externas Se guardan bajo llave (caja fuerte)
¿Se prevén medidas para garantizar los derechos y libertades de los interesados?	SI
En caso afirmativo, ¿cuáles?	• Procedimientos y canales para el ejercicio de derechos • Cláusulas informativas y base legitimadora para el tratamiento de datos

RESULTADO DEL ANÁLISIS

RIESGO MEDIO

NO ES NECESARIA EVALUACIÓN DE IMPACTO EN LA PROTECCIÓN DE DATOS

DOCUMENTO DE MEDIDAS DE SEGURIDAD

1. OBJETO Y FINALIDAD DEL DOCUMENTO

El presente documento y sus Anexos, redactados y englobados bajo el nombre de DOCUMENTO DE MEDIDAS DE SEGURIDAD, se crea para dar cumplimiento a lo dispuesto en el artículo 24 del RGPD (en relación al Considerando 74), así como satisfacer el principio de seguridad. Asimismo, el presente documento ¡recoge las medidas técnicas y organizativas necesarias para garantizar la protección, confidencialidad, integridad y disponibilidad de los sistemas de información de ISABEL BUEZO IBAÑEZ Y JOSE ANTONIO GOMEZ SAINZ DE LA MAZA CB.

Este documento es único y comprensivo de todos los tratamientos de ISABEL BUEZO IBAÑEZ Y JOSE ANTONIO GOMEZ SAINZ DE LA MAZA CB, y responde a las exigencias establecidas en relación a las medidas de seguridad. El documento deberá mantenerse en todo momento actualizado y ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo. El contenido del documento deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal. Dicho contenido mínimo es el siguiente (puesto que a día de hoy no existe Real Decreto que desarrolle la LOPDGDD, nos basaremos en el contenido recogido en el artículo 88.3 del RLOPD):

a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.

b) Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.

c) Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los datos.

d) Estructura de los datos con datos de carácter personal y descripción de los sistemas de información que los tratan.

e) Procedimiento de notificación, gestión y respuesta ante las incidencias.

f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los datos o tratamientos automatizados.

g) Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.

2. ÁMBITO DE APLICACIÓN DEL DOCUMENTO Y RECURSOS PROTEGIDOS

2.1. Ámbitos subjetivos y objetivos de aplicación

DATOS DE IDENTIFICACIÓN

Responsable del tratamiento	ISABEL BUEZO IBAÑEZ Y JOSE ANTONIO GOMEZ SAINZ DE LA MAZA CB
Número de identificación	J95720512
Dirección postal	GETXO, CL AMAIA 22 BJ, GETXO
Teléfono de contacto	944315467
Correo electrónico	oicarseleccion@gmail.com
Actividad realizada	AGENCIA DE COLOCACION

Este documento ha sido elaborado bajo la responsabilidad de ISABEL BUEZO IBAÑEZ Y JOSE ANTONIO GOMEZ SAINZ DE LA MAZA CB, quien, como responsable del tratamiento, se compromete a implantar y actualizar esta normativa de seguridad de obligado cumplimiento para todo el personal con acceso a los datos protegidos o a los sistemas de información que permiten el acceso a los mismos, incluyendo los sistemas de información, soportes y equipos empleados, departamentos, compartimentos, instalaciones y personal propio o ajeno que intervienen en el tratamiento y los locales en donde se ubican.

Por ello, todas las personas que tengan acceso a los datos, bien a través del sistema habilitado para acceder al mismo, o bien a través de cualquier otro medio automatizado de acceso, se encuentran obligadas por ley a cumplir lo establecido en este documento, y sujetas a las consecuencias que pudieran incurrir en caso de incumplimiento. Una copia de este documento será entregada o puesta a disposición, para su conocimiento, a cada persona

autorizada a acceder a los datos, siendo requisito obligatorio para poder acceder a esos datos el haber firmado la recepción del mismo.

Por todo ello, el responsable de los tratamientos y los encargados del tratamiento deberán implantar las medidas de seguridad con arreglo a lo dispuesto en el Título VIII del RLOPD, con independencia de cuál sea su sistema de tratamiento. Además, el presente documento será de aplicación a todos los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado. En cambio, no será aplicable a los tratamientos de datos referidos a personas jurídicas.

Asimismo, los datos relativos a empresarios individuales, cuando hagan referencia a ellos en su calidad de comerciantes, industriales o navieros, también se entenderán excluidos del régimen de aplicación de la protección de datos de carácter personal. Tampoco serán de aplicación los datos referidos a personas fallecidas. No obstante, las personas vinculadas al fallecido, por razones familiares o análogas, podrán dirigirse a los responsables del tratamiento que contengan datos de este con la finalidad de notificar el óbito, aportando acreditación suficiente del mismo, y solicitar, cuando hubiere lugar a ello, la cancelación de los datos.

2.2. Recursos protegidos

Se entiende por *recurso protegido* cualquier parte del sistema de información como son:

Locales de tratamiento y almacenamiento de datos: aquellas ubicaciones en donde se albergan los servidores, equipos informáticos, soportes… que contienen datos de carácter personal.

Servidores: dispositivos que contienen datos de carácter personal, incluyendo cualquier dispositivo informático que los almacena. Serán objeto de especial protección para garantizar la disponibilidad y confidencialidad de estos, principalmente cuando se acceda a los mismos desde una red de comunicaciones interna (Intranet) o externa (Red corporativa, Internet).

Equipos informáticos: dispositivos informáticos desde los cuales se puede acceder a datos de carácter personal.

Sistemas operativos y aplicaciones informáticas: programas o aplicaciones desde los que se puede acceder a datos personales y que son usualmente utilizados por los usuarios para acceder a dichos datos.

Soportes para copia y almacenamiento de datos: medios y canales de comunicación por el que circulan datos personales, a través de una red de comunicaciones interna o externa, serán objeto de especial protección, para garantizar la disponibilidad y confidencialidad de estos.

Datos automatizados: conjuntos de datos de carácter personal almacenados en soportes informáticos.

Datos no automatizados: conjuntos organizados de datos personales almacenados en soportes físicos.

La descripción de los recursos protegidos se detalla en el ANEXO I Recursos protegidos.

2.3. Definiciones

Para la correcta implantación de las medidas de carácter técnico y organizativo contenidas en el documento de medidas de seguridad, resulta necesario incluir las definiciones que nos da la normativa sobre los términos usados.

Datos de carácter personal: cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.

Tratamiento de datos: cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, modificación, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

Responsable del dato o del tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.

Afectado o interesado: persona física titular de los datos que sean objeto del tratamiento.

Encargado del tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del dato, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

Consentimiento del interesado: toda manifestación de voluntad, expresa, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

Cesión o comunicación de datos: tratamiento de datos que supone su revelación a una persona distinta del interesado.

Accesos autorizados: autorizaciones concedidas a un usuario para la utilización de los diversos recursos. En su caso, incluirán las autorizaciones o funciones que tenga atribuidas un usuario por delegación del responsable del dato o tratamiento o del responsable de seguridad.

Autenticación: procedimiento de comprobación de la identidad de un usuario.

Contraseña: información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario o en el acceso a un recurso.

Control de acceso: mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

Copia de respaldo: copia de los datos de un dato automatizado en un soporte que posibilite su recuperación.

Documento: todo escrito, gráfico, sonido, imagen o cualquier otra clase de información que puede ser tratada en un sistema de información como una unidad diferenciada.

Identificación: procedimiento de reconocimiento de la identidad de un usuario.

Incidencia: cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

Perfil de usuario: accesos autorizados a un grupo de usuarios.

Recurso: cualquier parte componente de un sistema de información.

Responsable de seguridad: persona o personas a las que el responsable del dato ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

Sistema de información: conjunto de datos, tratamientos, programas, soportes y en su caso, equipos empleados para el tratamiento de datos de carácter personal.

Sistema de tratamiento: modo en que se organiza o utiliza un sistema de información. Atendiendo al sistema de tratamiento, los sistemas de información podrán ser automatizados, no automatizados o parcialmente automatizados.

Soporte: objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos.

Transmisión de documentos: cualquier traslado, comunicación, envío, entrega o divulgación de la información contenida en el mismo. Usuario: sujeto o proceso autorizado para acceder a datos o recursos. Tendrán la consideración de usuarios los procesos que permitan acceder a datos o recursos sin identificación de un usuario físico.

3. MEDIDAS, NORMAS, PROCEDIMIENTOS, REGLAS Y ESTÁNDARES ENCAMINADOS A GARANTIZAR LOS NIVELES DE SEGURIDAD EXIGIDOS EN ESTE DOCUMENTO

El conjunto de medidas, normas, procedimientos y estándares, se adoptan teniendo en cuenta el RGPD y la LOPDGDD. Este documento deberá mantenerse permanentemente actualizado. Cualquier modificación relevante en los sistemas de información, en la organización de los mismos, o en las disposiciones vigentes en materia de seguridad de los datos de carácter personal conllevará la revisión de la normativa incluida y, si procede, su modificación total o parcial.

3.1 Centros de tratamiento y locales

Los locales donde se encuentran los equipos informáticos que contienen los datos objeto de tratamiento deben disponer de las medidas de seguridad mínimas al objeto de garantizar la confidencialidad de los datos de carácter personal y su disponibilidad. La ejecución de tratamiento de datos de carácter personal fuera de los locales de la ubicación del dato deberá ser autorizada expresamente por el responsable del tratamiento y, en todo caso, deberá garantizarse el nivel de seguridad correspondiente

En caso de que existan ordenadores portátiles con acceso a datos de carácter personal, estos tendrán que ser autorizados previamente a poder ser utilizados, siguiendo la política mencionada a continuación. Los empleados de la presente entidad, en el caso de que existan, que dispongan de ordenador portátil, serán informados de la prohibición, excepto de las excepciones autorizadas, de almacenar datos de carácter personal en el disco duro de los ordenadores portátiles y de la obligación de trabajar con datos de carácter personal únicamente sobre las unidades lógicas definidas en servidor o servidores de la empresa. Además, tendrán que cumplir con las medidas de seguridad implementadas en la entidad que quedan definidas en este documento.

Será obligatorio que en los ordenadores portátiles se habiliten los mismos criterios establecidos sobre identificación, autenticación y control de accesos definidos en este Documento de Seguridad, siempre que se conecten a la red local. Siempre que se tenga que acceder de forma remota a través de Redes de Comunicaciones, esta solo se podrá hacer si es una "conexión encriptada" de forma que todos los datos viajen por las Redes de Comunicaciones cifradas.

3.2 Puestos de trabajo

Se consideran puestos de trabajo todo ordenador personal, terminal u otro dispositivo desde el que se pueda acceder a los datos. Cada una de las personas autorizadas tendrá asignado un puesto de trabajo desde el que acceder a los datos. El usuario asignado al puesto de trabajo será responsable de garantizar que la información a la que accede no podrá ser visualizada o comunicada a personas no autorizadas. Cualquier dispositivo conectado al puesto de trabajo tales como impresoras o pantallas deberán de estar ubicadas de forma que se garantice la confidencialidad de la información y que esta no pueda ser visualizada o comunicada a personas no autorizadas

El usuario responsable del puesto de trabajo, cuando finalice su turno o cuando se ausente temporalmente, deberá dejar los equipos y dispositivos en un estado que impida

el acceso o la visualización de los datos protegidos a personas no autorizadas. Esto se podrá realizar mediante un protector de pantalla, la suspensión de la sesión de trabajo o la salida del sistema y apagado del equipo. La reanudación del trabajo implicará la desactivación de la pantalla protectora, el reinicio de la sesión o el encendido del equipo con la introducción del nombre de usuario y contraseña correspondiente en cada caso. No deberá dejar en la impresora documentos impresos en la bandeja de salida que contengan datos de carácter personal.

Si la impresora es compartida con otros usuarios no autorizados para acceder a los datos, el responsable de cada puesto de trabajo deberá retirar los documentos conforme vayan siendo impresos. La configuración de los puestos de trabajo desde los que se tiene acceso a los datos solo podrá ser cambiada con la autorización del responsable del tratamiento, el responsable de seguridad o el administrador del sistema designado.

3.3 Identificación y autenticación del personal autorizado

El responsable del tratamiento establecerá un procedimiento que garantice la correcta identificación y autenticación de los usuarios autorizados a acceder a los sistemas de información. Los accesos a los sistemas de información se realizarán mediante un mecanismo que permita la identificación de forma inequívoca y personalizada del usuario. Cada identificación deberá pertenecer a un único usuario.

3.3.1. Procedimiento de asignación y cambio de contraseñas.

El responsable del tratamiento o la persona con autorización delegada del responsable del tratamiento, asignará un nombre de usuario y propondrá una contraseña para cada uno de los usuarios que, tras el primer acceso, vendrán obligados a cambiarlas. Las contraseñas deberán constar de un mínimo de 6 dígitos y con una combinación de caracteres alfanuméricos. Se deberá evitar la utilización de nombre o cifras o su combinación que sean fácilmente deducibles. Las contraseñas se almacenarán de forma ininteligible. El archivo donde se almacenen las contraseñas deberá estar protegido y bajo la responsabilidad del administrador del sistema. Las contraseñas son de carácter personal e intransferible y no serán visibles en pantalla cuando son introducidas. Cada usuario será responsable de la confidencialidad de su contraseña y, en caso de que la misma sea conocida fortuita o fraudulentamente por personas no autorizadas, deberá registrarlo como incidencia y proceder inmediatamente a su cambio.

Con una periodicidad de cada 12 meses y de forma automática, se propondrá a los usuarios, que cambien su contraseña por una nueva, volviendo a quedar almacenada de forma ininteligible. El responsable del tratamiento o el administrador del sistema, en su caso, podrá cambiar los requisitos de acceso, las condiciones, modos sistemas y formas de tratamiento o de lectura cuando lo crea oportuno, notificando la decisión a los usuarios y dejando constancia de tal modificación en el Registro de incidencias. Las contraseñas personales constituyen uno de los componentes básicos de la seguridad de los datos, y deben por tanto estar especialmente protegidas. Como llaves de acceso al sistema, las contraseñas deberán ser estrictamente confidenciales y personales, y cualquier incidencia que comprometa su confidencialidad deberá ser inmediatamente comunicada al responsable del tratamiento o a la persona con autorización delegada del responsable del tratamiento y subsanada en el menor plazo de tiempo posible.

3.4 Control de acceso lógico

El RLOPD establece que los usuarios de los sistemas de información tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones. Si la aplicación informática que permite el acceso a los datos no cuenta con un control de acceso, deberá ser el sistema operativo, donde se ejecuta esa aplicación, el que impida el acceso no autorizado, mediante la restricción y disponibilidad de recursos en la sesión del usuario con el control de acceso lógico mediante usuario y contraseña. Queda prohibido que un usuario acceda a recursos con derechos distintos de los que ha sido autorizado.

En el caso de personal ajeno al responsable del tratamiento que tenga acceso a los recursos estará sometido a las mismas condiciones y obligaciones de seguridad que el personal propio. Exclusivamente la persona con autorización delegada del responsable tratamiento podrá conceder, alterar o anular el acceso autorizado sobre los datos y recursos, conforme a los criterios establecidos por el responsable del tratamiento. Para el caso de nuevas altas de accesos, se comunicará al responsable del tratamiento por la persona con autorización delegada, con la propuesta de acceso, código de acceso y listado de las funciones del nuevo autorizado.

3.5 Entorno de Sistema Operativo y de Comunicaciones

Al estar el dato de carácter personal ubicado en un ordenador (o con funciones de servidor) con un sistema operativo determinado y poder contar con unas conexiones que le comunican con otros ordenadores, es posible, para las personas que conozcan estos entornos, acceder a los datos protegidos sin pasar por los procedimientos de control de acceso con los que pueda contar la aplicación. El sistema operativo y de comunicaciones debe tener al menos un responsable o administrador. Ninguna herramienta o programa de utilidad que permita el acceso a los datos deberá ser accesible a ningún usuario o administrador no autorizado. Esto incluye cualquier medio de acceso en bruto no elaborado o editado a los datos que deberán estar bajo el control del administrador autorizado.

Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones, sean o no públicas, deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local. Si el ordenador en el que se ubica los datos está integrado en una red de comunicaciones de forma que desde otros ordenadores conectados a la misma sea posible el acceso al dato, el administrador responsable del sistema deberá asegurarse de que este acceso no se permite a personas no autorizadas.

3.6 Gestión de soportes y documentos

3.6.1. Etiquetado e Inventario de soportes

Los soportes que contengan datos de carácter personal deben ser etiquetados para permitir su identificación, conocer de qué datos se tratan y el tipo de información que contienen y la fecha de creación. El inventario de soportes deberá estar permanentemente actualizado. Se exceptúan estas obligaciones cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el documento de seguridad. La identificación de los soportes que contengan datos de carácter personal que la organización considere especialmente sensibles se podrá realizar utilizando sistemas de etiquetado que serán comprensibles y con significado para los usuarios con acceso autorizado a los citados soportes y documentos y que dificulten la identificación para el resto de personas.

3.6.2. Salida de soportes y documentos

La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del tratamiento, deberá ser autorizada por el responsable del tratamiento o la persona con autorización delegada del responsable del tratamiento o encontrarse debidamente autorizada en el documento de seguridad. Con respecto a los documentos también se consideran incluidos en la salida de documentos los siguientes supuestos:

- Envío por correo electrónico en el cuerpo del mensaje o como adjuntos datos de un tratamiento.
- Los faxes cuando incorporan datos de un o tratamiento.
- Cualquier otro procedimiento electrónico como FTP, descargas desde la web o carpetas compartidas…

Los ordenadores portátiles y los dispositivos móviles que contengan datos personales deberán de ser sometidos al mismo procedimiento de autorización para su salida de los locales en los que está ubicado el dato. La autorización de salida de soportes y documentos se gestiona mediante la hoja de autorización que se encuentra en el ANEXO II del presente documento de seguridad. En el caso del correo electrónico para garantizar la trazabilidad de los datos que salen materialmente del sistema de información, puede servir como registro el propio sistema de indexación del gestor del correo electrónico.

3.6.3. Traslado de soportes y documentación

En el traslado de la documentación se adoptarán las medidas y procedimientos apropiados para evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.

3.6.4. Destrucción y borrado de documentos o soportes

Aquellos soportes que se vayan a reutilizar deberán ser borrados físicamente antes de su reutilización, de forma que los datos que contenían no sean recuperables de ningún modo. No será válido el borrado lógico o rápido que impide el acceso a la información, pero no la elimina físicamente hasta que ha sobrescrito sobre la misma.

Los soportes que se vayan a eliminar deberán ser borrados físicamente antes de su eliminación, que consistirá en un proceso de destrucción mecánica del soporte, trituración o incineración. Los documentos en formato papel que vayan a desecharse, deberá procederse a su destrucción mediante la trituradora de papel. Está prohibida la reutilización de documentos en formato papel. Los procesos de reutilización y eliminación descritos han de ser previos a la preceptiva baja de los soportes en el inventario.

3.7 Datos temporales

Los datos temporales o copias de documentos que se hubiesen creado exclusivamente para la realización de trabajos temporales o auxiliares deberán cumplir el nivel de seguridad que les corresponde con arreglo a lo dispuesto en el RLOPD y la LOPDGDD y lo expresado en este documento. Los datos temporales o copias de documentos así creados serán borrados o destruidos una vez que hayan dejado de ser necesarios para los fines que motivaron su creación. Lo anterior, incluye los datos temporales que utilicen y generen las aplicaciones.

Las copias de trabajo de documentos en formato papel, deberá procederse a su destrucción mediante la trituradora de papel. Está prohibida la reutilización de documentos o copias de trabajo en formato papel. El responsable del tratamiento o, en su caso, el responsable de seguridad deberá asegurarse de que los datos temporales o copias de trabajo de documentos no son accesibles por personal no autorizado.

3.8 Criterios de archivo

El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y supresión, así como, en su caso, la limitación del tratamiento y portabilidad de los datos. En aquellos casos en los que no exista norma aplicable, el responsable del tratamiento deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo.

3.9 Dispositivos de almacenamiento y custodia de soportes

Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura. Cuando las características físicas de aquéllos no permitan adoptar esta medida, el responsable del tratamiento adoptará medidas que impidan el acceso de personas no autorizadas.

Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento indicados en el apartado anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

4. FUNCIONES Y OBLIGACIONES DEL PERSONAL

4.1 Obligaciones del Personal

La entidad deberá emitir un comunicado interno, en su caso, donde se establezcan las directrices para el tratamiento, por parte del personal, de los datos conocidos como consecuencia del desarrollo de su tarea dentro de la empresa. En este comunicado, se recogerán las principales obligaciones en materia de seguridad sobre datos de carácter personal incluyendo la prohibición expresa de instalar cualquier tipo de aplicación en los equipos informáticos y la utilización de recursos informáticos para otras finalidades diferentes de las estrictamente derivadas del desarrollo de su actividad laboral, así como la obligación de mantener el deber de secreto sobre todos los datos tratados con motivo del desarrollo de su puesto de trabajo y de no comunicar estos datos a ninguna persona o entidad sin la autorización pertinente. En concreto, el personal tendrá las siguientes obligaciones:

- Tratar los datos de carácter personal de conformidad con lo que se establece en la legislación vigente y en este documento, accediendo a ellos únicamente cuando sea necesario para el desarrollo de sus funciones.
- Mantener el secreto profesional respecto de los datos de carácter personal que se encuentran y custodiarlos. Esta obligación perdurará después de finalizar las relaciones con el responsable del tratamiento.
- Conocer la normativa interna en materia de seguridad, y especialmente la referente a protección de datos de carácter personal.

- Cumplir lo dispuesto en la normativa interna vigente en cada momento.
- Conocer las consecuencias que se pudieran derivar y las responsabilidades en que pudiera incurrir en caso de incumplimiento, que podrían derivar en sanciones.
- Comunicar al responsable del dato, en el mismo día, cualquier solicitud de ejercicio por parte de los afectados de los derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad.

De la misma forma, el usuario autorizado será el responsable de su puesto de trabajo, garantizando que la información que disponga o muestre su equipo no podrá ser accesible o visible por personas no autorizadas. Procurará que la disposición de pantallas e impresoras u otros dispositivos de su puesto de trabajo se ubiquen de forma que garanticen la confidencialidad y no sea accesible o visible su contenido por personas no autorizadas. Al abandonar su puesto de trabajo, aun temporalmente, deberá dejarlo en un estado que impida el acceso o la visualización de los datos protegidos, mediante un protector de pantalla o la salida del sistema y apagado del equipo. La reanudación del trabajo implicará la desactivación de la pantalla protectora o el encendido del equipo con la introducción del nombre de usuario y contraseña correspondiente en cada caso.

No deberá dejar en la impresora documentos impresos en la bandeja de salida que contengan datos protegidos. Si la impresora es compartida con otros usuarios no autorizados para acceder a los datos, el responsable de cada puesto de trabajo deberá retirar los documentos conforme vayan siendo impresos. La configuración de los puestos de trabajo desde los que se tiene acceso al dato sólo podrá ser cambiada con la autorización del responsable del tratamiento, el responsable de seguridad o el administrador del sistema designado.

Por otra parte, todo usuario es responsable de mantener la confidencialidad de su contraseña. Si la contraseña es conocida por otra persona, el usuario, deberá registrarlo como incidencia y notificarlo al responsable del tratamiento o al responsable de seguridad, para proceder a su cambio. El usuario que tenga conocimiento de una incidencia deberá de ponerlo en conocimiento del responsable del tratamiento o al responsable de seguridad y registrarla siguiendo el procedimiento establecido para el registro de incidencias. El conocimiento y la no notificación de una incidencia por parte de un usuario será considerado como una falta contra la seguridad por parte de ese usuario.

Los soportes informáticos que contengan datos han de estar claramente identificados con una etiqueta externa que indique el dato, tipo de datos y fecha de creación. Los soportes que sean reutilizables, y que hayan contenido copias de datos del dato, deberán ser borrados físicamente antes de su reutilización, de forma que los datos que contenían no sean recuperables. Los soportes que contengan datos del dato deberán ser almacenados en lugares a los que no tengan acceso personas que no sean autorizadas. La salida de equipos o soportes fuera de las instalaciones requiere la autorización del responsable del tratamiento o al responsable de seguridad. Además, tendrá que seguir los procedimientos establecidos de gestión y distribución de soportes y observar las autorizaciones precisas en cada caso.

Es más, no se podrá no utilizar el correo electrónico u otros medios de comunicación interna o con el exterior para transmitir mensajes que contengan o lleven adjuntos datos de carácter personal que por sus características, volumen o destinatarios puedan poner en peligro la confidencialidad o la integridad de los datos. Del mismo modo, tendrá que atenerse a los procedimientos establecidos y observar las autorizaciones precisas, y no realizar transferencias de datos con datos de carácter personal entre sistemas o descargas en equipos salvo en aquellos casos expresamente autorizados, y protegiendo después los contenidos para evitar la difusión o copias no autorizadas.

Finalmente, su obligación será proteger la confidencialidad e integridad de los datos personales de la entidad que excepcionalmente tuvieran que almacenarse o usarse fuera del lugar de trabajo: en casa del cliente, en el propio domicilio o en otras instalaciones alternativas tanto en sistemas fijos como en portátiles

4.2 Obligaciones encargadas al responsable del tratamiento

Con relación a las funciones establecidas en el RGPD al responsable del tratamiento, la Dirección tendrá que:

- Decidir sobre la finalidad, contenido y uso del tratamiento.
- Autorizar:
  - La ejecución de tratamientos de datos de carácter personal fuera de los locales de la ubicación del dato.
  - La salida de soportes informáticos que contengan datos de carácter personal fuera de los locales de la ubicación del dato.

- Realizar el control del tratamiento, calidad y seguridad de los datos.
- Controlar la gestión de soportes informáticos que contienen datos de carácter personal.
- Gestionar y dirigir los procedimientos de acceso, rectificación, cancelación y oposición, portabilidad y limitación de los datos de los afectados y resolver:
    - La petición de acceso en el plazo de un mes.
    - La petición de rectificación o cancelación en el plazo de 10 días.
- Proceder al bloqueo de los datos en los casos en que, siendo procedente su cancelación, no sea posible su extinción física, tanto por razones técnicas como por causa del procedimiento o soporte utilizado.
- Encargarse de que exista una relación actualizada de usuarios con acceso autorizado a los sistemas de información.
- Establecer los procedimientos de identificación y autenticación para dicho acceso. ·
- Establecer los mecanismos para evitar que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados.
- Establecer los procedimientos de realización de copias de respaldo y recuperación de datos.
- Encargarse de forma directa o por delegación del cumplimiento efectivo de la normativa sobre protección de datos en la organización, garantizando la difusión y conocimiento de este documento entre todo el personal.
- Implantar las medidas de seguridad establecidas en este documento.
- Mantener este documento actualizado en todo momento, debiendo revisarse siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo y adecuar su contenido a las disposiciones vigentes en materia de seguridad de datos.
- Garantizar los bienes jurídicos y recursos protegidos.

En resumen, se encargará de:

- Seguir fielmente lo descrito en el Apartado 11 Procedimiento de Revisión descrito más adelante.

- Establecer mecanismos para evitar que un usuario acceda a datos o recursos con derechos diferentes a los autorizados.
- Verificar la definición y correcta aplicación de los procedimientos de realización de copias de seguridad y recuperación de los datos.
- Establecer un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquél usuario que intente acceder al sistema de información y la verificación que está autorizado.
- Mantener una relación del personal autorizado para conceder, anular o alterar los derechos de acceso, conforme a los criterios establecidos.
- Mantener una relación del personal con acceso autorizado al lugar donde se almacenan los soportes.

5. ESTRUCTURA DE LOS REGISTROS DE ACTIVIDADES DE TRATAMIENTO Y SISTEMAS QUE LOS TRATAN

En el Registro de Actividades de Tratamiento, se contiene una descripción detallada de las categorías de datos que se tratan, con el contenido previsto en el artículo 30 RGPD.

6. RESPONSABLE DE SEGURIDAD

ISABEL BUEZO IBAÑEZ se designa Responsable de Seguridad y se encargará de coordinación y control de todas las medidas definidas en este documento. El Responsable de Seguridad desarrollará las funciones encargadas en tanto que no se nombre a otro diferente. En el ANEXO III Nombramiento del Responsable de Seguridad se encuentran copias del nombramiento del mismo.

7. REGISTRO DE INCIDENCIAS

ISABEL BUEZO IBAÑEZ Y JOSE ANTONIO GOMEZ SAINZ DE LA MAZA CB recogerá tantas incidencias de seguridad como se produzcan sobre los datos que trata. Se recogen en el ANEXO IV Registro de Incidencias la documentación sobre las incidencias que serán inexcusablemente registradas. Esta documentación podrá ser ampliada con otro tipo de incidencias que pudieran haber quedado omitidas.

Todos los empleados de la entidad han de ser conocedores de su obligación de comunicar las incidencias en materia de seguridad, tanto para los datos de carácter personal automatizados, como para los que se traten manualmente, al Responsable de Seguridad. Todas las comunicaciones tendrán que efectuarse al Responsable de Seguridad indicando el momento que se detectaron y utilizando el medio de comunicación más rápido, a ser posible personalmente o telefónicamente. El Responsable de Seguridad anotará en el Registro de Incidencias los siguientes datos:

- Tipo de incidencia.
- Momento en que se ha producido (fecha y hora).
- Persona que notificó la incidencia.
- Persona a la que se notifica.
- Efectos de la incidencia.
- Medidas correctoras adaptadas, en su caso.

El Responsable de Seguridad contactará con las personas oportunas para corregir la incidencia. Una vez observada su correcta resolución, registrará los efectos que se hayan producido como consecuencia de la misma.

8. NOTIFICACIÓN DE BRECHAS DE SEGURIDAD

Según el artículo 33 del RGPD, en caso de brechas de seguridad que afecten a los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente sin dilación indebida y, de ser posible, a más tardar en las 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha brecha de seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

Del mismo modo, el artículo 34 del RGPD, establece que cuando sea probable que la brecha de seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará a los afectados sin dilación indebida.

8.1 Notificación de brechas de seguridad

Tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una brecha de seguridad de los datos personales, debe, sin dilación y, a más

tardar en las 72 horas siguientes a tener constancia, efectuar la correspondiente notificación a la Autoridad de Control. Se considera que se tiene constancia de una brecha de seguridad cuando hay una certeza de que se ha producido y se tiene conocimiento suficiente de su naturaleza y alcance.

Para determinar si un incidente ha producido una "brecha de seguridad de los datos personales", el criterio a tener en cuenta recogido en el RGPD es "todas aquellas brechas de la seguridad que ocasiones la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos".

La comunicación se realizará con el modelo de comunicación contenido en el ANEXO V Formulario de notificación de incidentes de seguridad de datos personales. Y deberá contener la siguiente información:

Datos identificativos y de contacto de:

- Entidad/Responsable del tratamiento.
- Delegado de Protección de Datos (si está designado), o persona de contacto.
- Indicación de si se trata de una notificación completa o parcial. En caso de tratarse de notificación parcial, indicar si se trata de una primera notificación o una notificación complementaria.

Información sobre la brecha de seguridad de datos personales:

- Fecha y hora en la que se detecta.
- Fecha y hora en la que se produce el incidente y su duración.
- Circunstancias en que se haya producido la brecha de seguridad de datos personales (por ejemplo, pérdida, robo, copia, etc.).
- Naturaleza y contenido de los datos personales en cuestión.
- Resumen del incidente que ha causado la brecha de seguridad de datos personales (con indicación de la ubicación física y del soporte de almacenamiento).
- Posibles consecuencias y efectos negativos en los afectados.
- Medidas técnicas y organizativas que se hayan adoptado por parte del responsable del tratamiento.
- Categoría de los datos afectados y número de los registros afectados.
- Categoría y número de individuos afectados.
- Posibles cuestiones de carácter transfronterizo, indicando la posible necesidad de notificar a otras autoridades de control.

En caso de que no fuese posible facilitar toda la información en el momento de la notificación, podrá facilitarse posteriormente, de manera gradual en distintas fases. La primera notificación se realizará en las primeras 72 horas, y al menos se realizará una comunicación final o de cierre cuando se disponga de toda la información relativa al incidente.

Cuando el responsable realice la primera notificación, deberá informar si proporcionará más información a posteriori. También podrá aportar información adicional mediante comunicaciones intermedias a la autoridad de control bajo petición de ésta, o cuando el responsable considere adecuado actualizar la situación de la misma.

Cuando la notificación inicial no sea posible en el plazo de 72 horas, la notificación deberá realizarse igualmente, y en ella deberán constar y justificarse los motivos de la dilación.

8.2 Identificación de la autoridad de control

Si el incidente afecta a los datos de personas en más de un Estado miembro, el responsable deberá realizar una evaluación sobre cuál es la autoridad principal a la que deberá realizar la notificación y, en caso de duda, se debe como mínimo, notificar a la autoridad de control local donde la brecha ha tenido lugar. Actuará como autoridad de control principal la del establecimiento principal o la del único establecimiento del responsable. Los criterios para identificar el establecimiento principal son:

- Lugar donde tenga la sede principal el responsable.
- Lugar donde se toman las decisiones sobre fines y medios.

La notificación a la AEPD se realizará a través del formulario destinado a tal efecto publicado en la sede electrónica de la agencia, en https://sedeagpd.gob.es/sede-electronica-web/, cuyo modelo se incluye en el ANEXO V Formulario de notificación de incidentes de seguridad de datos personales. A cada notificación se le asignará una referencia que el responsable deberá mantener e incluir en las sucesivas comunicaciones relacionadas si las hubiera, con el fin de proporcionar un seguimiento completo del incidente.

8.3 Proceso de comunicación al afectado

Existen diversos factores a tener en cuenta para decidir si se ha de realizar la comunicación a las personas afectadas:

- Cuáles son las obligaciones legales y contractuales.
- Riesgos que comporta la pérdida de los datos: daños físicos, daños reputacionales, etc.
- Existe un riesgo razonable de suplantación de identidad o fraude en función del tipo de información que se ha visto afectada y teniendo en cuenta si la información estaba seudonimizada o cifrada.
- Hasta qué punto la persona afectada puede evitar o mitigar posibles daños posteriores.

Si después del análisis correspondiente es necesario realizar la notificación, pero se prevé que la comunicación a los afectados puede comprometer el resultado de una investigación en curso, la comunicación podría posponerse siempre bajo la supervisión de la autoridad de control. La comunicación a los afectados se realizará a la mayor brevedad posible, en un lenguaje claro y sencillo y siempre en estrecha cooperación con la autoridad de control y las autoridades policiales, de acuerdo con sus orientaciones. El contenido mínimo de esta comunicación será el siguiente:

- Datos de contacto del Delegado de Protección de Datos o, en su caso, del punto de contacto en el que pueda obtenerse más información.
- Descripción general del incidente y momento en que se ha producido.
- Las posibles consecuencias de la brecha de la seguridad de los datos personales.
- Descripción de los datos e información personal afectados.
- Resumen de las medidas implantadas hasta el momento para controlar los posibles daños.
- Otras informaciones útiles a los afectados para proteger sus datos o prevenir posibles daños.

La notificación se deberá realizar, preferentemente, de forma directa al afectado, ya sea por teléfono, correo electrónico, SMS, a través de correo postal, o a través de cualquier

otro medio dirigido al afectado que el responsable considere adecuado. La notificación indirecta, a través de avisos públicos en sitios web como blogs corporativos, o comunicados de prensa, se utilizará cuando para la notificación directa los costos sean excesivos o cuando no sea posible contactar con las personas afectadas (por ejemplo, porque se desconocen, o los datos de contacto no están actualizados).

8.4 Excepciones a la notificación / comunicación

La notificación a la autoridad de control no será necesaria cuando el responsable pueda demostrar, de forma fehaciente, que la brecha de la seguridad de los datos personales no entraña un riesgo para los derechos y las libertades de las personas físicas. Por ejemplo, si los datos ya se encontraban públicamente disponibles y su revelación no entraña ningún riesgo hacia el titular de los datos. Tampoco será necesaria la comunicación a los afectados cuando:

- El responsable ha tomado medidas técnicas y organizativas adecuadas, como que los datos no sean inteligibles para personas o máquinas no autorizadas con anterioridad a la brecha de seguridad de datos personales (mediante el uso de cifrados de datos de última generación, minimización, disociación de datos, acceso a entornos de prueba sin datos reales, etc.). Por ejemplo, es probable que no sea necesaria la notificación si se pierde un dispositivo móvil y los datos personales que contiene están cifrados. Sin embargo, sí que es posible que se requiera de notificación si ésta fuera la única copia de los datos personales o, por ejemplo, la clave de cifrado en posesión del responsable estuviera comprometida
- El responsable ha tomado con posterioridad a la brecha de seguridad de datos personales las medidas de protección que mitiguen total o parcialmente el posible impacto para los afectados y garanticen que ya no hay posibilidad de que el alto riesgo se materialice. Por ejemplo, mediante la identificación y puesta en marcha inmediatamente de las medidas contra la persona que ha accedido a los datos personales antes de que pudieran hacer algo con ellos
- Cuando la notificación a los afectados suponga un esfuerzo desproporcionado a nivel técnico y organizativo. Por ejemplo, cuando los detalles de contacto se hayan perdido como resultado de la brecha, o aquellos casos en los que se tenga que desarrollar un nuevo sistema o proceso para realizar la notificación, o se requiera la dedicación

excesiva de recursos internos para la identificación de los afectados. Ante esta situación, se realizará la notificación de manera pública a través de los canales establecidos por el responsable.

Si el responsable todavía no ha comunicado al afectado la brecha de seguridad de los datos personales considerando el alto riesgo potencial, la autoridad de control podrá exigirle:

- Que lo comunique.
- Podrá decidir que se cumpla alguna de las condiciones mencionadas para que la comunicación a los afectados no sea obligada.

9. PROCEDIMIENTOS DE COPIAS DE SEGURIDAD Y RECUPERACIÓN

Es obligatorio establecer procedimientos de actuación para la realización como mínimo semanal de copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos. Por otra parte, los procedimientos para la recuperación de los datos deben garantizar en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

9.1 Procedimiento de realización de copias de respaldo

El responsable se encargará de realizar al menos un tipo de copia de seguridad que se relacionan a continuación:

Copia de seguridad digital ***Copia SEMANAL***

Así mismo, se exigirá a los terceros encargados del tratamiento la realización de copias de seguridad con una periodicidad igual o inferior a las descritas en este apartado. Las copias de respaldo deberán conservarse en un lugar diferente de aquél donde se encuentren los equipos informáticos que los tratan.

9.2 Procedimiento de Recuperación de datos

Los procedimientos para la recuperación de los datos deben garantizar en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción. La entidad tendrá en cuenta si la recuperación pone en riesgo la disponibilidad de las aplicaciones, para lo cual trasladará una pregunta al respecto al tercero que presta el servicio de mantenimiento de las aplicaciones y en función de su respuesta solicitará instrucciones precisas sobre cómo realizar dicha recuperación o bien podrá solicitar a dicha empresa de mantenimiento la prestación de este servicio de restauración.

En el caso de situaciones que no supongan un riesgo para la disponibilidad de las aplicaciones, se tendrá que seguir inexcusablemente los siguientes pasos:

- Cumplimentación de una solicitud por parte del peticionario que tendrá que contar con el beneplácito el Responsable de Seguridad.
- Se procederá a trasladar la orden de recuperación al personal autorizado, enviando copia al peticionario indicando la aprobación o denegación de dicha restauración.
- El Responsable de Seguridad anotará el hecho en el Registro de Resolución de Incidencias.
- Toda la documentación original será archivada por el Responsable de Seguridad.

9.3. Verificación de los procedimientos de copia y recuperación de datos

El responsable del tratamiento o la persona con autorización delegada del responsable del tratamiento verificará cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y recuperación de los datos.

9.4. Pruebas con datos reales

Las pruebas anteriores a la implantación o modificación de los sistemas de información no se realizarán con datos reales, salvo que previamente se haya realizado una copia de seguridad y se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote su realización en el documento de seguridad. De las pruebas realizadas conforme al párrafo anterior, deberá quedar constancia en el registro de incidencias. Sin embargo, la entidad no dispone de un entorno de desarrollo y pruebas

independientes del entorno de explotación. Todas las pruebas anteriores a la implantación o modificaciones de los sistemas de información se realizan dotándolas de todas las medidas de seguridad incluidas en este documento.

10. PROCEDIMIENTO DE REVISIÓN

10.1 Revisión del Documento de Seguridad

El documento de seguridad deberá mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los tratamientos o, en su caso, como consecuencia de los controles periódicos realizados. En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

El contenido del documento de seguridad deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal. El responsable del tratamiento o la persona con autorización delegada del responsable del dato o tratamiento, junto con el responsable de seguridad, si es el caso, mantendrán un reunión con carácter ordinario cada seis meses y con carácter extraordinario cada vez que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los datos o tratamientos, con el objetivo de coordinar los cambios a introducir en el documento de seguridad, elevando conclusiones al responsable del tratamiento.

10.2 Análisis de riesgos

Con la finalidad de medir los riesgos y amenazas a los que se enfrenta la entidad, se elabora el Análisis de Riesgos. Así mismo el responsable del tratamiento deberá llevar a cabo una revisión del Análisis de riesgos o, en su caso, la sustitución del mismo, cuando tenga lugar un cambio en las actividades de tratamiento de datos personales, todo ello con el objeto de poder adoptar las medidas de control y seguridad para garantizar los derechos y libertades de los interesados. El responsable de seguridad será el encargado de revisar el Análisis de riesgos y lo elevará al responsable del tratamiento. El Análisis de riesgos

se archivará junto o anexado al documento de seguridad y estará a disposición de la Agencia Española de Protección de Datos.

11. CONSECUENCIAS DEL INCUMPLIMIENTO DEL DOCUMENTO DE SEGURIDAD

El incumplimiento de las obligaciones y medidas de seguridad establecidas en el presente documento por el personal afectado se sancionará conforme a las disposiciones disciplinarias en materia de protección de datos.

ANEXOS AL DOCUMENTO DE SEGURIDAD

ANEXO I. RECURSOS PROTEGIDOS

LOCALES DE TRATAMIENTO Y ALMACENAMIENTO DE DATOS

Responsable del tratamiento	ISABEL BUEZO IBAÑEZ Y JOSE ANTONIO GOMEZ SAINZ DE LA MAZA CB
Número de identificación	J95720512
Dirección postal	GETXO, CL AMAIA 22 BJ
Teléfono de contacto	944315467
Correo electrónico	oicarseleccion@gmail.com
Actividad realizada	AGENCIA DE COLOCACION

INVENTARIO DE EQUIPOS INFORMÁTICOS DE SOBREMESA, PORTÁTILES, IMPRESORAS…

Código	**Tipo de Hardware: Ordenador Personal**

Sistema Operativo: Fabricante: Uso: Dispositivo Portátil: Sistema de Cifrado: Sistema de etiquetado:	Descripción: Modelo: Fecha:
Código	**Tipo de Hardware: Impresora**
Sistema Operativo: Fabricante: Uso: Dispositivo Portátil: Sistema de Cifrado: Sistema de etiquetado:	Descripción: Modelo: Fecha:
Medidas de seguridad de los equipos	Control de acceso a los equipos (usuario y contraseña personalizados) Sistema de autenticación (contraseñas personalizadas)

INVENTARIO DE SISTEMAS OPERATIVOS Y APLICACIONES INFORMÁTICAS

Aplicación	Descripción	Fecha de consulta
ADOBE ACROBAT	Lector de documentos PDF	
CORREO ELECTRÓNICO	Prestador de servicios de comunicaciones electrónicas y almacenamiento de datos	
MICROSOFT OFFICE	*Software* de ofimática	

Red local (LAN) y Wi-Fi	Control de acceso a la red local y sistemas cifrados de seguridad de las redes Wi-Fi. Existe conexión remota.	

SOPORTES PARA COPIA O ALMACENAMIENTO DE INFORMACIÓN

Aplicación	Medidas de seguridad	Fecha de consulta
Software de copias de respaldo	Ubicación de la copia: se guardan bajo llave y en caja fuerte. Periodicidad de la back up: semanal, como mínimo. Comprobación: máximo 6 meses desde la creación. Cifrado: sí.	

ANEXO II. FORMULARIO DE ENTRADA Y SALIDA DE SOPORTES

ENTRADA DE SOPORTES

Datos del soporte	Datos de entrada	Emisor	Firma
Código del soporte: Tipo de soporte: Fecha de Copia: Contenido:	Responsable de recepción: Fecha y hora: Periodicidad: Número de soportes: Forma de envío:	Empresa: Persona: Motivo:	

SALIDA DE SOPORTES

Datos del soporte	Datos de salida	Destinatario	Firma
Código del soporte:	Responsable de entrega:	Empresa:	

Tipo de soporte: Fecha de Copia: Contenido:	Fecha y hora: Periodicidad: Remitente: Forma de envío: Salida autorizada por:	Persona: Motivo:	

ANEXO III. NOMBRAMIENTO DEL RESPONSABLE DE SEGURIDAD Y RELACIÓN DE PERSONAL AUTORIZADO

NOMBRAMIENTO DEL RESPONSABLE DE SEGURIDAD

En Getxo, a 20 de mayo de 2021

De acuerdo con el Reglamento (UE) 6016/679, 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) y la legislación española en materia de protección de datos de carácter personal, se nombra a ISABEL BUEZO IBAÑEZ **Responsable de Seguridad**, haciéndose cargo de las tareas relacionadas a continuación:

1. Actualizar el presente documento y adecuación del mismo a la normativa vigente;
2. Cumplir y hacer cumplir todas las obligaciones, funciones y medidas establecidas en el presente documento.

En prueba de conformidad, ambas partes firman el presente documento por duplicado y a un solo efecto, en el lugar y fecha “ut supra”.

ANEXO IV. REGISTRO DE INCIDENCIAS

El Registro de Incidencias será mantenido exclusivamente por el Responsable de Seguridad. Se facilitará el acceso únicamente a quien lo tenga que consultar para realizar análisis encaminado al estudio de acciones a llevar a cabo para la resolución de las incidencias. Así mismo, el Registro de Incidencias tiene que ser obligatoriamente consultado por los auditores en ejercicio de sus funciones.

Incidencia Nº: |____|	
Fecha de notificación:	
Tipo de incidencia:	
Descripción detallada de la incidencia:	
Fecha y hora en que se produjo la incidencia:	
Persona(s) a quien(es) se comunica:	
Efectos que puede producir: (en caso de no subsanación o incluso independientemente de ella)	
Recuperación de Datos: (a rellenar sólo si la incidencia es de este tipo) Procedimiento realizado: Datos restaurados: Datos grabados manualmente: Persona que ejecutó el proceso:	

Firma del responsable de seguridad: Fdo _____
Persona que realiza la comunicación: Fdo.:_____

ANEXO V. FORMULARIO DE NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD DE DATOS PERSONALES

Se trata de un documento oficial. Para acceder al mismo, acceda a: https://www.aepd.es/media/guias/guia-brechas-seguridad.pdf (vid. página 49).

ANEXO VI. MODIFICACIONES INTRODUCIDAS EN LAS REVISIONES DE ESTE DOCUMENTO

Versión	Fecha	Actualizaciones
V.1		Realización inicial del documento

ANEXOS AL DOCUMENTO

ANEXO I. CLÁUSULA DE PROTECCIÓN DE DATOS PARA LAS FACTURAS Y PRESUPUESTOS

En cumplimiento con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, 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), le comunicamos que los datos que usted nos facilita han sido incorporados en la base de datos de ISABEL BUEZO IBAÑEZ Y JOSE ANTONIO GOMEZ DE LA MAZA CB, con el fin de poderle prestar nuestros servicios. Los datos proporcionados se conservarán mientras se mantenga la relación comercial o durante los años necesarios para cumplir con las obligaciones legales. Los datos bancarios se cederán únicamente en aquellos casos en los que exista una obligación legal.

Usted tiene derecho a acceder a sus datos personales, rectificar los datos inexactos o solicitar su supresión cuando los datos ya no sean necesarios, así como, en su caso, a la limitación del tratamiento y portabilidad de sus datos, pudiendo ejercitarlos dirigiendo un escrito a la dirección que figura en el encabezamiento de esta factura. De la misma forma ISABEL BUEZO IBAÑEZ Y JOSE ANTONIO GOMEZ DE LA MAZA CB, se compromete a tratar de forma confidencial los datos de carácter personal facilitados y a no comunicar o ceder dicha información a terceros.

ANEXO II. COLETILLA CORREO ELECTRÓNICO

Se debería incluir en la firma del correo electrónico.

CORTA:

En cumplimiento del RGPD y la LOPDGDD le comunicamos que su dirección de correo electrónico forma parte de la base de datos de ISABEL BUEZO IBAÑEZ Y JOSE ANTONIO GOMEZ DE LA MAZA CB, con la única finalidad de mantener comunicaciones. En cualquier momento podrá ejercer sus derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad de los datos en la siguiente dirección de correo electrónico: oicarseleccion@gmail.com

La información contenida en este correo electrónico o en cualquier dato anexo al mismo tiene carácter CONFIDENCIAL, exclusivamente dirigida a su destinatario y es propiedad de ISABEL BUEZO IBAÑEZ Y JOSE ANTONIO GOMEZ SAINZ DE LA MAZA CB, quedando prohibida su divulgación, copia o distribución a terceros sin su previa autorización escrita. En caso de haber recibido este correo electrónico por error, por favor, contacte con el remitente del mensaje para su reenvío y proceda a destruirlo.

LARGA:

En cumplimiento de la Ley 34/2002 de la Sociedad de la Información y de Comercio Electrónico y del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, 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 – a partir de ahora, RGPD-), le comunicamos que su dirección de correo electrónico forma parte de la base de datos de ISABEL BUEZO IBAÑEZ Y JOSE ANTONIO GOMEZ SAINZ DE LA MAZA CB con la única finalidad de mantener comunicaciones.

En virtud de lo dispuesto en el artículo 15 y siguientes del RGPD, en cualquier momento usted podrá ejercer sus derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad de los datos, dirigiéndose por escrito a: oicarseleccion@gmail.com. La solicitud deberá contener el nombre y apellidos del interesado, fotocopia del D.N.I. (o, en su caso, pasaporte o C.I.F.), petición en que se concreta la solicitud, domicilio a efectos de notificaciones, fecha, firma y documentos acreditativos de la petición que se formula. Los modelos se pueden encontrar en https://www.aepd.es/reglamento/derechos/index.html.

Además, en cumplimiento de lo prevenido en el artículo 21 de la Ley 34/2002 de Servicios de la Sociedad de la Información y Comercio Electrónico, si usted no desea recibir más información sobre nuestros servicios puede darse de baja en la siguiente dirección de correo electrónico: oicarseleccion@gmail.com, indicando en el asunto "baja" o "no enviar correos".

Finalmente, la información contenida en este correo electrónico y, en su caso, en cualquier dato anexo al mismo tiene carácter confidencial, está exclusivamente dirigida a su destinatario o destinatarios y es propiedad de ISABEL BUEZO IBAÑEZ Y JOSE ANTONIO GOMEZ SAINZ DE LA MAZA CB. Queda prohibida su divulgación, copia o distribución a terceros sin la previa autorización escrita de ISABEL BUEZO IBAÑEZ, en virtud de la legislación vigente.

En caso de haber recibido este correo electrónico por error, por favor, contacte con el remitente del mensaje para su reenvío y proceda a destruirlo.

ANEXO III. COMPROMISO DE CONFIDENCIALIDAD SIN ACCESO A DATOS

En Getxo, a 2021

REUNIDOS

DE UNA PARTE, ISABEL BUEZO IBAÑEZ en nombre y representación de ISABEL BUEZO IBAÑEZ Y JOSE ANTONIO GOMEZ SAINZ DE LA MAZA CB, en adelante, el "CLIENTE", con número de identificación J95720512 y domicilio social en GETXO, CL AMAIA 22 BJ.

DE OTRA PARTE, D. XXXX, mayor de edad, con D.N.I. número XXXXX y en su propio nombre, en adelante, el "PROVEEDOR", con domicilio profesional en XXXXX

El CLIENTE y el PROVEEDOR, en adelante, podrán ser denominadas, individualmente, "la Parte" y, conjuntamente, "las Partes", reconociéndose mutuamente capacidad jurídica y de obrar suficiente para la celebración del presente Contrato.

EXPONEN

PRIMERO: Que el CLIENTE ha contratado al PROVEEDOR los servicios de PONER.

SEGUNDO: Que el CLIENTE ha adoptado las medidas adecuadas para limitar el acceso del personal a los datos de carácter personal, a los soportes que los contengan o a los recursos de los sistemas de información, para la realización de trabajos que no impliquen tratamiento de datos personales. Todo ello en conformidad con la normativa de protección de datos.

Que las Partes reunidas en la sede social del CLIENTE, acuerdan celebrar el presente contrato de CONFIDENCIALIDAD, en adelante, el "Contrato", de acuerdo con las siguientes

CLÁUSULAS

ÚNICA. – NO ACCESO A DATOS DE CARÁCTER PERONAL Y DEBER DE CONFIDENCIALIDAD

En virtud del presente Contrato, el PROVEEDOR se obliga a no acceder a datos personales que se encuentren alojados en los equipos del CLIENTE, ya sean automatizados o no. En todo caso, cuando fuese imprescindible el mero acceso provisional para la prestación del servicio, se obliga a acceder única y exclusivamente a aquellos datos que sean estrictamente necesarios para la prestación del servicio, y a no apropiarse ni hacer suyos de modo alguno, o a alojar en sus propios equipos o copiar manualmente, ni ceder a terceros, los datos del CLIENTE a los que hubiera accedido.

Asimismo, se obliga a mantener secreto y confidencialidad acerca de los datos del CLIENTE a los que pudiera acceder a fin de que se lleve a cabo la prestación de los servicios contratados. Este deber de confidencialidad será exigible durante la prestación de servicios y subsistirá una vez finalizado el mismo.

Y en prueba de cuanto antecede, las Partes suscriben el Contrato, en dos ejemplares y a un solo efecto, en el lugar y fecha señalados en el encabezamiento

EL CLIENTE EL PROVEEDOR

Fdo.: _____ Fdo.: _____

*Es un contrato a suscribir por las personas que lleven a cabo un contrato de prestación de servicios sin acceso a datos (por ejemplo, sería un contrato a firmar con el personal de limpieza o mensajería)

ANEXO IV. CONTRATO DE PRESTACIÓN DE SERVICIOS (ENCARGO DE TRATAMIENTO DE DATOS)

REUNIDOS

DE UNA PARTE, ISABEL BUEZO IBAÑEZ, en nombre y representación de ISABEL BUEZO IBAÑEZ Y JOSE ANTONIO GOMEZ SAINZ DE LA MAZA CB, en adelante, el "RESPONSABLE", con número de identificación J95720512 y domicilio social en GETXO, CL AMAIA 22 BJ.

DE OTRA PARTE y en adelante, el "ENCARGADO", XXXXXX con número de identificación XXXXX y domicilio social en XXXXX, actuando en su nombre y representación D./Dª. XXX, mayor de edad y con DNI XXXXX

EXPONEN

1. Que ambas partes se reconocen capacidad legal necesaria para contratar y suscribir el presente contrato, de conformidad con el artículo 28 del Reglamento (UE) 2016/679, de 27 de abril de 2016, del Parlamento Europeo y del Consejo relativo a la Protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de los mismos (en adelante, "RGPD").
2. Que el RESPONSABLE ha contratado los servicios del ENCARGADO que se detallan a continuación.
3. Ambas partes convienen en aceptar el presente Contrato de acuerdo a las siguientes

CLÁUSULAS

1.- Objeto del encargo del tratamiento

El presente contrato tiene por objeto definir las condiciones conforme a las cuales el Encargado llevará a cabo el tratamiento de datos personales necesario para la correcta prestación de los Servicios XXXXX

Las operaciones de tratamiento autorizadas serán las estrictamente necesarias para alcanzar la finalidad del encargo incluyendo, si se precisa, la recogida, registro, estructuración, modificación, conservación, extracción, consulta, comunicación por transmisión, difusión, interconexión, cotejo, limitación, supresión y destrucción de datos.

En el caso de que la prestación de servicios implique recogida de datos personales, el Encargado cumplirá el deber de información conforme a las instrucciones que le sean facilitadas por el Responsable y, en cualquier caso, deberá facilitar previamente, como mínimo, la información requerida de acuerdo a lo establecido en el artículo 13 del RGPD.

2.- Identificación de la información afectada

Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, el responsable del tratamiento pone a disposición del encargado del tratamiento, en su caso, la siguiente información: nombre, apellidos, dirección postal, correo electrónico, dirección bancaria, entre otros. Todos los datos que se recaban son los estrictamente necesarios para la prestación del servicio.

3.- Duración

La duración del presente acuerdo será conforme a la duración de la relación contractual que mantengan el RESPONSABLE y el ENCARGADO. Una vez finalice el presente contrato, el encargado del tratamiento debe devolver al responsable y suprimir cualquier copia que esté en su poder. No obstante, podrá mantener bloqueados los datos para atender posibles responsabilidades administrativas o jurisdiccionales.

4.- Obligaciones del encargado del tratamiento

El encargado del tratamiento y todo su personal se obliga a:

a. Utilizar los datos personales objeto de tratamiento, o los que recoja para su inclusión, sólo para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para fines propios.

b. Tratar los datos de acuerdo con las instrucciones del responsable del tratamiento. Si el encargado del tratamiento considera que alguna de las instrucciones infringe el RGPD o

cualquier otra disposición en materia de protección de datos de la Unión o de los Estados miembros, el encargado informará inmediatamente al responsable.

c. Llevar, por escrito, un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable (cuando proceda), que contenga:

   i. El nombre y los datos de contacto del encargado y de cada responsable por cuenta del cual actúe el encargado y, en su caso, del representante del responsable o del encargado y del delegado de protección de datos (si procede).

   ii. Las categorías de tratamientos efectuados por cuenta de cada responsable.

   iii. En su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49 apartado 1, párrafo segundo del RGPD, la documentación de garantías adecuadas.

   iv. Una descripción general de las medidas técnicas y organizativas de seguridad relativas a:

      a) La seudonimización y el cifrado de datos personales.

      b) La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

      c) La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.

      d) El proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

d. No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del responsable del tratamiento, en los supuestos legalmente admisibles. El encargado puede comunicar los datos a otros encargados del tratamiento del mismo responsable, de acuerdo con las instrucciones del responsable. En este caso, el responsable identificará, de forma previa y por escrito, la entidad a la que se deben comunicar los datos, los datos a comunicar y las medidas de seguridad a aplicar para proceder a la comunicación. Si el encargado debe transferir datos personales a un tercer país o a una organización internacional, en virtud del

Derecho de la Unión o de los Estados miembros que le sea aplicable, informará al responsable de esa exigencia legal de manera previa, salvo que tal Derecho lo prohíba por razones importantes de interés público.

e. Si fuera necesario subcontratar algún tratamiento, este hecho se deberá comunicar previamente y por escrito al responsable, con una antelación de quince días, indicando los tratamientos que se pretende subcontratar e identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto. La subcontratación podrá llevarse a cabo si el responsable no manifiesta su oposición en el plazo establecido.

   El subcontratista, que también tendrá la condición de encargado del tratamiento, está obligado igualmente a cumplir las obligaciones establecidas en este documento para el encargado del tratamiento y las instrucciones que dicte el responsable. Corresponde al encargado inicial regular la nueva relación de forma que el nuevo encargado quede sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad…) y con los mismos requisitos formales que él, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas. En el caso de incumplimiento por parte del subencargado, el encargado inicial seguirá siendo plenamente responsable ante el responsable en lo referente al cumplimiento de las obligaciones.

f. Mantener el deber de secreto respecto a los datos de carácter personal a los que haya tenido acceso en virtud del presente encargo, incluso después de que finalice su objeto.

g. Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de las que hay que informarles convenientemente.

h. Mantener a disposición del responsable la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.

i. Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.

j. Cuando las personas afectadas ejerzan los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones individualizadas automatizadas ante el encargado de tratamiento, éste debe comunicarlo por correo electrónico a la dirección que indique el responsable de tratamiento. La comunicación debe hacerse de forma inmediata y en ningún caso más allá del día laborable siguiente al de

la recepción de la solicitud, juntamente, en su caso, con otras informaciones que puedan ser relevantes para resolver la solicitud.

k. El responsable de tratamiento deberá facilitar el derecho de información en el momento de la recogida de los datos.

l. Notificación de violaciones de la seguridad de los datos. El encargado del tratamiento notificará al responsable del tratamiento, sin dilación indebida, y en cualquier caso antes del plazo de 48h (margen para cumplir con las 72h de plazo máximo establecido), y a través de correo electrónico correspondiente, las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia

No será necesaria la notificación cuando sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si se dispone de ella se facilitará, como mínimo, la información siguiente:

a) Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.

b) El nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.

c) Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.

d) Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos. Si no es posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

Corresponde al encargado del tratamiento, a petición del responsable de tratamiento, comunicar las violaciones de la seguridad de los datos a la Autoridad de Protección de Datos. La comunicación contendrá, como mínimo, la información siguiente:

a) Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.

b) Nombre y datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.

c) Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.

d) Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Si no es posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

m. Dar apoyo al responsable del tratamiento en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando proceda.

n. Dar apoyo al responsable del tratamiento en la realización de las consultas previas a la autoridad de control, cuando proceda.

o. Poner disposición del responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen el responsable u otro auditor autorizado por él.

p. Implantar las medidas de seguridad técnicas y organizativas necesarias para garantizar la seguridad de los datos tratados. En todo caso, deberá implantar mecanismos para:

a) Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

b) Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.

c) Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.

d) Seudonimizar y cifrar los datos personales, en su caso.

q. Cuando proceda, designar un delegado de protección de datos y comunicar su identidad y datos de contacto al responsable.

r. En el caso de que finalice la prestación del servicio, respecto a los datos, el encargado deberá: Devolver al RESPONSABLE los datos de carácter personal y, si procede, los soportes donde consten, una vez cumplida la prestación, conforme y según las normas sectoriales de aplicación. El ENCARGADO puede conservar una copia, con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

5.- Obligaciones del responsable del tratamiento

Corresponde al responsable del tratamiento:

a. Entregar al encargado los datos a los que se refiere la cláusula 2 de este Contrato.

b. Realizar un análisis de los posibles riesgos derivados del tratamiento para determinar las medidas de seguridad apropiadas para garantizar la seguridad de la información tratada y los derechos y libertades de los interesados y, si se determinara que existen riesgos, realizar una evaluación de impacto para que se proceda a la implementación de medidas adecuadas para evitarlos o mitigarlos.

c. Realizar las consultas previas que corresponda.

d. Velar, de forma previa y durante todo el tratamiento, por el cumplimiento del RGPD por parte del encargado.

e. Supervisar el tratamiento, incluida la realización de inspecciones y auditorías.

6.- Validez

En el caso de que alguna o algunas de las cláusulas del presente contrato pasen a ser inválidas, ilegales o inejecutables en virtud de alguna norma jurídica, se considerarán ineficaces en la medida que corresponda, pero en lo demás, este contrato conservará su validez.

7.- Fuero y jurisdicción

Con renuncia a su fuero y domicilio, todas las partes se someten, expresa y formalmente, a la jurisdicción de los Tribunales de Salamanca para toda cuestión que pueda surgir en la interpretación o aplicación del presente contrato.

Y para que así conste a todos los efectos lo firman, en prueba de conformidad las partes que intervienen y sin tener más que consignar, por duplicado y a un sólo efecto en el lugar y fecha indicado.

RESPONSABLE DEL TRATAMIENTO ENCARGADO DE TRATAMIENTO

Firma. Firma

*** Este contrato de encargo del tratamiento debe firmarse con todos aquellos a los que se les ceden contratos. Por lo general, se suele anexar al contrato de prestación de servicios. En este contrato, se recoge la forma, finalidad, etc. del tratamiento de los datos de los clientes.

ANEXO V. FORMULARIO PARA RECOGIDA DE DATOS BÁSICOS

Se comunica que, de conformidad con el Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27 de abril, sus datos personales se incluirán en la base de datos de ISABEL BUEZO IBAÑEZ Y JOSE ANTONIO GOMEZ SAINZ DE LA MAZA CB. Los datos no se cederán a

terceros, salvo que sea necesario para prestar el servicio o para satisfacer eventuales responsabilidades legales y administrativas. Al mismo tiempo, los datos se conservarán por el tiempo mínimo necesario para la prestación del servicio y, en su caso, para satisfacer eventuales reclamaciones administrativas o judiciales.

Las finalidades legítimas del tratamiento de los datos de carácter personal a los que hacemos referencia son atender las posibles relaciones que puedan surgir entre el usuario y el prestador de servicio, concretamente y sin carácter taxativo, contratación de servicios, envío de presupuestos, contestar a su solicitud, tramitar su petición o mantener la relación contractual/precontractual; y realizar comunicaciones sobre productos y/o servicios que pudieran ser de interés,

Podrá ejercer en cualquier momento sus derechos reconocidos en el Reglamento General de Protección de Datos de acceso, rectificación y supresión de sus datos personales, así como también puede solicitar la portabilidad de los mismos, oponerse al tratamiento y solicitar la limitación de este, en este último caso únicamente se conservarán para el ejercicio o la defensa de reclamaciones. El cliente puede ejercer dichos derechos dirigiéndose mediante un escrito al local ubicado en GETXO, CL AMAIA 22 BJ o mediante correo electrónico, a través de la dirección oicarseleccion@gmail.com

En caso de que el cliente considere que sus datos no se atienden de manera correcta, tiene derecho a presentar una reclamación ante la Agencia Española de Protección de Datos, cuyos datos de contacto son: Teléfonos: 901.100. 099 91.266.35.17; Dirección Postal: C/ Jorge Juan, 6, 28001-Madrid; Sede Electrónica: https://sedeagpd.gob.es/sede-electronica-web/ y página web: www.agpd.es .

☐ Consiento el tratamiento de mis datos de carácter personal con las finalidad de prestar el servicio.

☐ Consiento el tratamiento de mis datos de carácter personal con las finalidad de recibir comunicaciones publicitarias.

Firmado:

*Debe incluirse en la hoja de encargo de los servicios profesionales o en el contrato de prestación de servicios.

** La casilla no puede estar premarcada, siendo obligatoria rellenarla, puesto que sin ella no habría consentimiento para tratar los datos del cliente.

ANEXO VI. FORMULARIO PARA RECOGIDA DE DATOS SENSIBLES

INFORMACIÓN BÁSICA SOBRE PROTECCIÓN DE DATOS

Responsable del tratamiento	ISABEL BUEZO IBAÑEZ Y JOSE ANTONIO GOMEZ SAINZ DE LA MAZA CB CIF: J95720512 Teléfono de contacto: (+34) 944315467 Dirección de contacto principal: Getxo, Cl Amaia 22 Bj Correo electrónico: oicarseleccion@gmail.com
Finalidad del tratamiento	Por lo general, prestación de servicios
Legitimación	Ejecución de un contrato
Derechos	Acceder, rectificar y suprimir los datos, así como otros derechos, como se explica en la información adicional
Procedencia de los datos	Datos obtenidos de los propios clientes No se compran datos a terceros
Información adicional	A continuación, podrá leerla

INFORMACIÓN ADICIONAL

En cumplimiento con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, 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 o RGPD), se comunica que:

- En nombre de la empresa tratamos la información que nos facilita con el fin de prestarles el servicio solicitado y poder ofrecerle productos y servicios de acuerdo con sus intereses. La cesión de sus datos será necesaria para poder prestarles dicho servicio, no pudiendo prestarlo en caso de que no proporcione sus datos.
- Los datos proporcionados se conservarán mientras se mantenga la relación comercial o de prestación de servicios, o durante los años necesarios para cumplir con las obligaciones legales.

- Los datos personales que tratamos proceden del propio interesado o de terceros legitimados para la cesión de los mismos.
- Los datos se cederán, en su caso, a terceras personas, para el cumplimiento de obligaciones legales o con la finalidad de mantener una relación comercial con usted, o en los casos en que fuera imprescindible para la correcta prestación del servicio. En cualquier caso, no se cederán sus datos a terceros países.
- La entidad cumple con el principio de confidencialidad exigido por la normativa vigente y, asimismo, garantiza el cumplimiento de todos los mecanismos de seguridad para la protección de sus datos de carácter personal.
- Usted tiene derecho a obtener confirmación sobre si en nuestra entidad estamos tratando sus datos personales por tanto tiene derecho a solicitar del responsable el acceso a sus datos personales, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos. También tendrá derecho a presentar una reclamación ante la autoridad de control.
- El ejercicio de los derechos se deberá realizar mediante envío de comunicación escrita a la dirección Getxo, Calle Amaia 22 Bk, o bien mediante escrito al correo electrónico oicarseleccion@gmail.com. La solicitud deberá contener el nombre y apellidos del interesado, fotocopia del D.N.I. (o, en su caso, pasaporte o C.I.F.), petición en que se concreta la solicitud, domicilio a efectos de notificaciones, fecha, firma y documentos acreditativos de la petición que se formula. Los modelos se pueden encontrar en https://www.aepd.es/reglamento/derechos/index.html.
- Los datos de carácter personal recogidos por nuestra entidad serán conservados durante el tiempo que sea necesario conforme a la finalidad del tratamiento de los mismos, cumpliendo en todo caso con los plazos legalmente preceptivos exigidos por la normativa aplicable.

☐ Consiento el tratamiento de mis datos de carácter personal con las finalidad de prestar el servicio

☐ Consiento el tratamiento de mis datos de carácter personal con las finalidad de recibir comunicaciones publicitarias.

FECHA

NOMBRE Y APELLIDOS

FIRMA

***¿Cómo ofrecer esta información?

Dos posibilidades:

- En el mismo formulario cumplimentado (por ejemplo, en el reverso)
- Como un anexo o separata que se entregue al interesado

ANEXO VII. ACUSE DE RECIBO DE CV

En primer lugar, le agradecemos el interés que ha mostrado por dirigirse a OICAR SELECCION al enviarnos su currículum vitae.

Le informamos que, de conformidad con la normativa sobre protección de datos, sus datos serán objeto de tratamiento por ISABEL BUEZO IBAÑEZ Y JOSE ANTONIO GOMEZ SAINZ DE LA MAZA CB como responsable del mismo con la finalidad de gestionar su currículum para la selección de personal. Si su perfil no se ajustase a los requisitos buscados en los vigentes procesos de selección procederemos a conservar sus datos para futuros procesos que sí se acomoden a su perfil, salvo que Vd. nos manifestara lo contrario. Su CV será conservado hasta el mes de octubre de cada año independientemente de su llegada.

Contamos con su consentimiento para el tratamiento de los datos que nos ha facilitado, de forma voluntaria, libre e informada al enviarnos su CV al correo electrónico habilitado a tal efecto.

Por otro lado, queremos comunicarle que no cederemos sus datos a terceros, salvo autorización expresa u obligación. Tampoco están previstas transferencias internacionales a terceros países.

Podrá ejercer sus derechos de acceso, rectificación, supresión, oposición, limitación al tratamiento, portabilidad, transparencia en la información y a no ser objeto de decisiones individualizadas automatizadas (incluida la elaboración de perfiles), comunicándolo por escrito, ante esta misma empresa a Getxo, Calle Amaia 22 Bj, o mediante el envío de un correo electrónico a oicarseleccion@gmail.com , adjuntando una fotocopia del DNI o documento similar acreditativo de su identidad.

Sin otro particular, aprovechamos la ocasión para enviarle un cordial saludo.

Atentamente,

XXXX

ANEXO VIII. CONTRATO DE CONFIDENCIALIDAD CON EMPLEADOS

En cumplimiento del 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") le informamos de los siguientes extremos:

Responsable del tratamiento: sus datos pasarán a formar parte de la base de datos de ISABEL BUEZO IBAÑEZ Y JOSE ANTONIO GOMEZ SAINZ DE LA MAZA CB, con domicilio social en Getxo, Cl Amaia 22 Bj.

Finalidad del tratamiento de sus datos:

- El empleado declara que facilita voluntariamente estos datos para el mantenimiento y cumplimiento de la relación, así como para llevar a cabo las gestiones de personal, contable y administrativa de la empresa.
- Recursos humanos: desarrollar, mantener, cumplir y controlar su actividad, y dar cumplimiento a las obligaciones y funciones del departamento de RECURSOS HUMANOS relativas a las actividades de formación, control de asistencia al trabajo, formalización de las nóminas, deberes en materia de prevención de riesgos laborales, así como la gestión de canales de comunicación/denuncias implementadas por la entidad de

conformidad con requisitos previstos en las normativas en materia de cumplimientos vigentes.

- Derechos de imagen: utilización de su imagen para la elaboración de publicaciones internas, y para su utilización con finalidades de marketing y prospección comercial de la entidad, así como a la publicación de su CV e información de su trayectoria profesional en nuestra Intranet, Webs, Redes Sociales y blogs corporativos. En ningún caso estas imágenes e información de carácter personal serán cedidas a terceros, ni utilizadas para una finalidad distinta a la descrita.

Legitimación: se basa en el contrato laboral suscrito con ISABEL BUEZO IBAÑEZ Y JOSE ANTONIO GOMEZ DE LA MAZA CB

Destinatarios: para el cumplimiento de las obligaciones legales, sus datos podrán ser comunicados a:

- Administraciones Públicas (Seguridad Social, Agencia Tributaria, Subvenciones, etc.)
- Mutuas de protección laboral y servicios de prevención de riesgos laborales o la preservación de la salud de los trabajadores.
- Aquellas entidades o clientes que exijan o ante las cuales sea necesario identificar a los empleados: entidades bancarias para el pago de nóminas, aseguradoras, proyectos, formación, mensajería, renting, identificación de infracciones de tráfico, así como aquellas entidades o clientes que requieran datos identificativos y laborales del personal para llevar a cabo el servicio contratado y que acrediten la relación con la empresa.
- Comités de empresa, sindicatos y delegados de prevención.
- Asesoría laboral, si existiese.

Sus datos no serán cedidos para otras finalidades distintas a las descritas.

Derechos. Queda informado de que tiene derecho a obtener confirmación sobre si en ISABEL BUEZO IBAÑEZ Y JOSE ANTONIO GOMEZ DE LA MAZA CB estamos tratando sus datos personales por tanto tiene derecho a solicitar del responsable el acceso a sus datos personales, y su rectificación o supresión, y, en su caso, el derecho a la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos (en cuyo caso

únicamente serán conservados para el cumplimiento de las obligaciones legalmente previstas). También tendrá derecho a presentar una reclamación ante la autoridad de control y a revocar su autorización para el uso de sus imágenes.

El ejercicio de los derechos se deberá realizar dirigiéndose a la siguiente dirección: Getxo, Calle Amaia 22 Bj CB

COMPROMISO DE CONFIDENCIALIDAD

D./Dña. NOMBRE Y APELLIDOS trabajador, con D.N.I. XXXXXX, en el marco de la relación laboral que le une con xxxx empresa, se compromete a:

- No revelar a ninguna persona ajena a OICAR SELECCION, sin el consentimiento debido, información a la que haya tenido acceso en el desarrollo de sus funciones, excepto en aquellos casos en los que sea necesario para dar el debido cumplimiento a sus obligaciones o por habérsele requerido por mandato legal o de la autoridad competente.
- Utilizar la información que se menciona en el apartado anterior únicamente en la forma que exige el desarrollo de sus funciones en OICAR SELECCION y a no utilizarla de otra forma o finalidad.
- No utilizar de ninguna otra manera cualquier información que haya podido obtener utilizando su condición de empleado y que no sea necesaria para el desarrollo de sus funciones.
- Cumplir, en el desarrollo de sus funciones, la normativa vigente relativa a la Protección de Datos de Carácter Personal, y en particular, el RGPD o cualquier otra norma que las sustituya o modifique en el futuro, así como la legislación nacional relativa a protección de datos.
- No utilizar ni incorporar a los sistemas informáticos y archivos documentales de esta entidad la información de carácter personal o empresarial a la que haya tenido acceso durante el desempeño de sus tareas o funciones en otras entidades, cuando ello pueda implicar la vulneración de las legislaciones mencionadas.
- Cumplir los compromisos anteriores aun cuando se extinga, por cualquier causa, la relación laboral que le une a ISABEL BUEZO IBAÑEZ Y JOSE ANTONIO GOMEZ DE LA MAZA CB

- Guardar secreto profesional respecto de los datos personales, datos sobre los clientes, estrategias comerciales y organizativas e industriales, y cualquier otra información a la que tenga acceso con el motivo de las funciones asignadas.
- El empleado declara así mismo conocer que el incumplimiento de este compromiso puede generar el ejercicio de acciones disciplinarias por parte de ISABEL BUEZO IBAÑEZ Y JOSE ANTONIO GOMEZ DE LA MAZA CB, tal como establece el artículo 58 del Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.

De igual modo, le informamos que, con la finalidad de garantizar el derecho a la intimidad y privacidad del trabajador por parte de ISABEL BUEZO IBAÑEZ Y JOSE ANTONIO GOMEZ DE LA MAZA CB, bajo ningún concepto usted debe incorporar a los sistemas informáticos y archivos documentales de esta entidad, su información de carácter personal tales como fotos, vídeos o imágenes.

En el caso de producirse alguna modificación de sus datos, el empleado se compromete a comunicarlo por escrito, con la finalidad de mantener los datos actualizados.

LUGAR Y FECHA

Firma del empleado

ANEXOS AL DOCUMENTO

ANEXO I. CLÁUSULA DE PROTECCIÓN DE DATOS PARA LAS FACTURAS Y PRESUPUESTOS

En cumplimiento con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, 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), le comunicamos que los datos que usted nos facilita han sido incorporados en la base de datos de ISABEL BUEZO IBAÑEZ Y JOSE ANTONIO GOMEZ DE LA MAZA CB, con el fin de poderle prestar nuestros servicios. Los datos proporcionados se conservarán mientras se mantenga la relación comercial o durante los años necesarios para cumplir con las obligaciones legales. Los datos bancarios se cederán únicamente en aquellos casos en los que exista una obligación legal.

Usted tiene derecho a acceder a sus datos personales, rectificar los datos inexactos o solicitar su supresión cuando los datos ya no sean necesarios, así como, en su caso, a la limitación del tratamiento y portabilidad de sus datos, pudiendo ejercitarlos dirigiendo un escrito a la dirección que figura en el encabezamiento de esta factura. De la misma forma ISABEL BUEZO IBAÑEZ Y JOSE ANTONIO GOMEZ DE LA MAZA CB, se compromete a tratar de forma confidencial los datos de carácter personal facilitados y a no comunicar o ceder dicha información a terceros.

ANEXO II. COLETILLA CORREO ELECTRÓNICO

Se debería incluir en la firma del correo electrónico.

CORTA:

En cumplimiento del RGPD y la LOPDGDD le comunicamos que su dirección de correo electrónico forma parte de la base de datos de ISABEL BUEZO IBAÑEZ Y JOSE ANTONIO GOMEZ DE LA MAZA CB, con la única finalidad de mantener comunicaciones. En cualquier momento podrá ejercer sus derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad de los datos en la siguiente dirección de correo electrónico: oicarseleccion@gmail.com

La información contenida en este correo electrónico o en cualquier dato anexo al mismo tiene carácter CONFIDENCIAL, exclusivamente dirigida a su destinatario y es propiedad de ISABEL BUEZO IBAÑEZ Y JOSE ANTONIO GOMEZ SAINZ DE LA MAZA CB, quedando prohibida su divulgación, copia o distribución a terceros sin su previa autorización escrita. En caso de haber recibido este correo electrónico por error, por favor, contacte con el remitente del mensaje para su reenvío y proceda a destruirlo.

LARGA:

En cumplimiento de la Ley 34/2002 de la Sociedad de la Información y de Comercio Electrónico y del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, 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 – a partir de ahora, RGPD-), le comunicamos que su dirección de correo electrónico forma parte de la base de datos de ISABEL BUEZO IBAÑEZ Y JOSE ANTONIO GOMEZ SAINZ DE LA MAZA CB con la única finalidad de mantener comunicaciones.

En virtud de lo dispuesto en el artículo 15 y siguientes del RGPD, en cualquier momento usted podrá ejercer sus derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento y portabilidad de los datos, dirigiéndose por escrito a: oicarseleccion@gmail.com. La solicitud deberá contener el nombre y apellidos del interesado, fotocopia del D.N.I. (o, en su caso, pasaporte o C.I.F.), petición en que se concreta la solicitud, domicilio a efectos de notificaciones, fecha, firma y documentos acreditativos de la petición que se formula. Los modelos se pueden encontrar en https://www.aepd.es/reglamento/derechos/index.html.

Además, en cumplimiento de lo prevenido en el artículo 21 de la Ley 34/2002 de Servicios de la Sociedad de la Información y Comercio Electrónico, si usted no desea recibir más información sobre nuestros servicios puede darse de baja en la siguiente dirección de correo electrónico: oicarseleccion@gmail.com, indicando en el asunto "baja" o "no enviar correos".

Finalmente, la información contenida en este correo electrónico y, en su caso, en cualquier dato anexo al mismo tiene carácter confidencial, está exclusivamente dirigida a su destinatario o

ANEXO III. COMPROMISO DE CONFIDENCIALIDAD SIN ACCESO A DATOS

En Getxo, a 2021

REUNIDOS

DE UNA PARTE, ISABEL BUEZO IBAÑEZ en nombre y representación de ISABEL BUEZO IBAÑEZ Y JOSE ANTONIO GOMEZ SAINZ DE LA MAZA CB, en adelante, el "CLIENTE", con número de identificación J95720512 y domicilio social en GETXO, CL AMAIA 22 BJ.

DE OTRA PARTE, D. XXXX, mayor de edad, con D.N.I. número XXXXX y en su propio nombre, en adelante, el "PROVEEDOR", con domicilio profesional en XXXXX

El CLIENTE y el PROVEEDOR, en adelante, podrán ser denominadas, individualmente, "la Parte" y, conjuntamente, "las Partes", reconociéndose mutuamente capacidad jurídica y de obrar suficiente para la celebración del presente Contrato.

EXPONEN

PRIMERO: Que el CLIENTE ha contratado al PROVEEDOR los servicios de PONER.

SEGUNDO: Que el CLIENTE ha adoptado las medidas adecuadas para limitar el acceso del personal a los datos de carácter personal, a los soportes que los contengan o a los recursos de los sistemas de información, para la realización de trabajos que no impliquen tratamiento de datos personales. Todo ello en conformidad con la normativa de protección de datos.

Que las Partes reunidas en la sede social del CLIENTE, acuerdan celebrar el presente contrato de CONFIDENCIALIDAD, en adelante, el "Contrato", de acuerdo con las siguientes

CLÁUSULAS

ÚNICA. – NO ACCESO A DATOS DE CARÁCTER PERONAL Y DEBER DE CONFIDENCIALIDAD

En virtud del presente Contrato, el PROVEEDOR se obliga a no acceder a datos personales que se encuentren alojados en los equipos del CLIENTE, ya sean automatizados o no. En todo caso, cuando fuese imprescindible el mero acceso provisional para la prestación del servicio, se obliga a acceder única y exclusivamente a aquellos datos que sean estrictamente necesarios para la prestación del servicio, y a no apropiarse ni hacer suyos de modo alguno, o a alojar en sus propios equipos o copiar manualmente, ni ceder a terceros, los datos del CLIENTE a los que hubiera accedido.

Asimismo, se obliga a mantener secreto y confidencialidad acerca de los datos del CLIENTE a los que pudiera acceder a fin de que se lleve a cabo la prestación de los servicios contratados. Este deber de confidencialidad será exigible durante la prestación de servicios y subsistirá una vez finalizado el mismo.

Y en prueba de cuanto antecede, las Partes suscriben el Contrato, en dos ejemplares y a un solo efecto, en el lugar y fecha señalados en el encabezamiento

EL CLIENTE EL PROVEEDOR

Fdo.: _____ Fdo.: _____

*Es un contrato a suscribir por las personas que lleven a cabo un contrato de prestación de servicios sin acceso a datos (por ejemplo, sería un contrato a firmar con el personal de limpieza o mensajería)

ANEXO IV. CONTRATO DE PRESTACIÓN DE SERVICIOS (ENCARGO DE TRATAMIENTO DE DATOS)

REUNIDOS

DE UNA PARTE, ISABEL BUEZO IBAÑEZ, en nombre y representación de ISABEL BUEZO IBAÑEZ Y JOSE ANTONIO GOMEZ SAINZ DE LA MAZA CB, en adelante, el "RESPONSABLE", con número de identificación J95720512 y domicilio social en GETXO, CL AMAIA 22 BJ.

DE OTRA PARTE y en adelante, el "ENCARGADO", XXXXXX con número de identificación XXXXX y domicilio social en XXXXX, actuando en su nombre y representación D./Dª. XXX, mayor de edad y con DNI XXXXX

EXPONEN

1. Que ambas partes se reconocen capacidad legal necesaria para contratar y suscribir el presente contrato, de conformidad con el artículo 28 del Reglamento (UE) 2016/679, de 27 de abril de 2016, del Parlamento Europeo y del Consejo relativo a la Protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de los mismos (en adelante, "RGPD").

2. Que el RESPONSABLE ha contratado los servicios del ENCARGADO que se detallan a continuación.
3. Ambas partes convienen en aceptar el presente Contrato de acuerdo a las siguientes

CLÁUSULAS

1.- Objeto del encargo del tratamiento

El presente contrato tiene por objeto definir las condiciones conforme a las cuales el Encargado llevará a cabo el tratamiento de datos personales necesario para la correcta prestación de los Servicios XXXXX

Las operaciones de tratamiento autorizadas serán las estrictamente necesarias para alcanzar la finalidad del encargo incluyendo, si se precisa, la recogida, registro, estructuración, modificación, conservación, extracción, consulta, comunicación por transmisión, difusión, interconexión, cotejo, limitación, supresión y destrucción de datos.

En el caso de que la prestación de servicios implique recogida de datos personales, el Encargado cumplirá el deber de información conforme a las instrucciones que le sean facilitadas por el Responsable y, en cualquier caso, deberá facilitar previamente, como mínimo, la información requerida de acuerdo a lo establecido en el artículo 13 del RGPD.

2.- Identificación de la información afectada

Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, el responsable del tratamiento pone a disposición del encargado del tratamiento, en su caso, la siguiente información: nombre, apellidos, dirección postal, correo electrónico, dirección bancaria, entre otros. Todos los datos que se recaban son los estrictamente necesarios para la prestación del servicio.

3.- Duración

La duración del presente acuerdo será conforme a la duración de la relación contractual que mantengan el RESPONSABLE y el ENCARGADO. Una vez finalice el presente contrato, el encargado del tratamiento debe devolver al responsable y suprimir cualquier

copia que esté en su poder. No obstante, podrá mantener bloqueados los datos para atender posibles responsabilidades administrativas o jurisdiccionales.

4.- Obligaciones del encargado del tratamiento

El encargado del tratamiento y todo su personal se obliga a:

a. Utilizar los datos personales objeto de tratamiento, o los que recoja para su inclusión, sólo para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para fines propios.

b. Tratar los datos de acuerdo con las instrucciones del responsable del tratamiento. Si el encargado del tratamiento considera que alguna de las instrucciones infringe el RGPD o cualquier otra disposición en materia de protección de datos de la Unión o de los Estados miembros, el encargado informará inmediatamente al responsable.

c. Llevar, por escrito, un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable (cuando proceda), que contenga:

i. El nombre y los datos de contacto del encargado y de cada responsable por cuenta del cual actúe el encargado y, en su caso, del representante del responsable o del encargado y del delegado de protección de datos (si procede).

ii. Las categorías de tratamientos efectuados por cuenta de cada responsable.

iii. En su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49 apartado 1, párrafo segundo del RGPD, la documentación de garantías adecuadas.

iv. Una descripción general de las medidas técnicas y organizativas de seguridad relativas a:

a) La seudonimización y el cifrado de datos personales.

b) La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

c) La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.

d) El proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

d. No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del responsable del tratamiento, en los supuestos legalmente admisibles. El encargado puede comunicar los datos a otros encargados del tratamiento del mismo responsable, de acuerdo con las instrucciones del responsable. En este caso, el responsable identificará, de forma previa y por escrito, la entidad a la que se deben comunicar los datos, los datos a comunicar y las medidas de seguridad a aplicar para proceder a la comunicación. Si el encargado debe transferir datos personales a un tercer país o a una organización internacional, en virtud del Derecho de la Unión o de los Estados miembros que le sea aplicable, informará al responsable de esa exigencia legal de manera previa, salvo que tal Derecho lo prohíba por razones importantes de interés público.

e. Si fuera necesario subcontratar algún tratamiento, este hecho se deberá comunicar previamente y por escrito al responsable, con una antelación de quince días, indicando los tratamientos que se pretende subcontratar e identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto. La subcontratación podrá llevarse a cabo si el responsable no manifiesta su oposición en el plazo establecido.

El subcontratista, que también tendrá la condición de encargado del tratamiento, está obligado igualmente a cumplir las obligaciones establecidas en este documento para el encargado del tratamiento y las instrucciones que dicte el responsable. Corresponde al encargado inicial regular la nueva relación de forma que el nuevo encargado quede sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad…) y con los mismos requisitos formales que él, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas. En el caso de incumplimiento por parte del subencargado, el

encargado inicial seguirá siendo plenamente responsable ante el responsable en lo referente al cumplimiento de las obligaciones.

f. Mantener el deber de secreto respecto a los datos de carácter personal a los que haya tenido acceso en virtud del presente encargo, incluso después de que finalice su objeto.

g. Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de las que hay que informarles convenientemente.

h. Mantener a disposición del responsable la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.

i. Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.

j. Cuando las personas afectadas ejerzan los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones individualizadas automatizadas ante el encargado de tratamiento, éste debe comunicarlo por correo electrónico a la dirección que indique el responsable de tratamiento. La comunicación debe hacerse de forma inmediata y en ningún caso más allá del día laborable siguiente al de la recepción de la solicitud, juntamente, en su caso, con otras informaciones que puedan ser relevantes para resolver la solicitud.

k. El responsable de tratamiento deberá facilitar el derecho de información en el momento de la recogida de los datos.

l. Notificación de violaciones de la seguridad de los datos. El encargado del tratamiento notificará al responsable del tratamiento, sin dilación indebida, y en cualquier caso antes del plazo de 48h (margen para cumplir con las 72h de plazo máximo establecido), y a través de correo electrónico correspondiente, las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia

No será necesaria la notificación cuando sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si se dispone de ella se facilitará, como mínimo, la información siguiente:

a) Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.

b) El nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.

c) Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.

d) Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos. Si no es posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

Corresponde al encargado del tratamiento, a petición del responsable de tratamiento, comunicar las violaciones de la seguridad de los datos a la Autoridad de Protección de Datos. La comunicación contendrá, como mínimo, la información siguiente:

a) Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.

b) Nombre y datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.

c) Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.

d) Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Si no es posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

m. Dar apoyo al responsable del tratamiento en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando proceda.

n. Dar apoyo al responsable del tratamiento en la realización de las consultas previas a la autoridad de control, cuando proceda.

o. Poner disposición del responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen el responsable u otro auditor autorizado por él.

p. Implantar las medidas de seguridad técnicas y organizativas necesarias para garantizar la seguridad de los datos tratados. En todo caso, deberá implantar mecanismos para:

a) Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

b) Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.

c) Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.

d) Seudonimizar y cifrar los datos personales, en su caso.

q. Cuando proceda, designar un delegado de protección de datos y comunicar su identidad y datos de contacto al responsable.

r. En el caso de que finalice la prestación del servicio, respecto a los datos, el encargado deberá: Devolver al RESPONSABLE los datos de carácter personal y, si procede, los soportes donde consten, una vez cumplida la prestación, conforme y según las normas sectoriales de aplicación. El ENCARGADO puede conservar una copia, con

los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

5.- Obligaciones del responsable del tratamiento

Corresponde al responsable del tratamiento:

a. Entregar al encargado los datos a los que se refiere la cláusula 2 de este Contrato.

b. Realizar un análisis de los posibles riesgos derivados del tratamiento para determinar las medidas de seguridad apropiadas para garantizar la seguridad de la información tratada y los derechos y libertades de los interesados y, si se determinara que existen riesgos, realizar una evaluación de impacto para que se proceda a la implementación de medidas adecuadas para evitarlos o mitigarlos.

c. Realizar las consultas previas que corresponda.

d. Velar, de forma previa y durante todo el tratamiento, por el cumplimiento del RGPD por parte del encargado.

e. Supervisar el tratamiento, incluida la realización de inspecciones y auditorías.

6.- Validez

En el caso de que alguna o algunas de las cláusulas del presente contrato pasen a ser inválidas, ilegales o inejecutables en virtud de alguna norma jurídica, se considerarán ineficaces en la medida que corresponda, pero en lo demás, este contrato conservará su validez.

7.- Fuero y jurisdicción

Con renuncia a su fuero y domicilio, todas las partes se someten, expresa y formalmente, a la jurisdicción de los Tribunales de Salamanca para toda cuestión que pueda surgir en la interpretación o aplicación del presente contrato.

Y para que así conste a todos los efectos lo firman, en prueba de conformidad las partes que intervienen y sin tener más que consignar, por duplicado y a un sólo efecto en el lugar y fecha indicado.

RESPONSABLE DEL TRATAMIENTO ENCARGADO DE TRATAMIENTO

Firma. Firma

*** Este contrato de encargo del tratamiento debe firmarse con todos aquellos a los que se les ceden contratos. Por lo general, se suele anexar al contrato de prestación de servicios. En este contrato, se recoge la forma, finalidad, etc. del tratamiento de los datos de los clientes.

ANEXO V. FORMULARIO PARA RECOGIDA DE DATOS BÁSICOS

Se comunica que, de conformidad con el Reglamento UE 2016/679 del Parlamento Europeo y del Consejo de 27 de abril, sus datos personales se incluirán en la base de datos de ISABEL BUEZO IBAÑEZ Y JOSE ANTONIO GOMEZ SAINZ DE LA MAZA CB. Los datos no se cederán a terceros, salvo que sea necesario para prestar el servicio o para satisfacer eventuales responsabilidades legales y administrativas. Al mismo tiempo, los datos se conservarán por el tiempo mínimo necesario para la prestación del servicio y, en su caso, para satisfacer eventuales reclamaciones administrativas o judiciales.

Las finalidades legítimas del tratamiento de los datos de carácter personal a los que hacemos referencia son atender las posibles relaciones que puedan surgir entre el usuario y el prestador de servicio, concretamente y sin carácter taxativo, contratación de servicios, envío de presupuestos, contestar a su solicitud, tramitar su petición o mantener la relación contractual/precontractual; y realizar comunicaciones sobre productos y/o servicios que pudieran ser de interés,

Podrá ejercer en cualquier momento sus derechos reconocidos en el Reglamento General de Protección de Datos de acceso, rectificación y supresión de sus datos personales, así como también puede solicitar la portabilidad de los mismos, oponerse al tratamiento y solicitar la limitación de este, en este último caso únicamente se conservarán para el ejercicio o la defensa de reclamaciones. El cliente puede ejercer dichos derechos dirigiéndose mediante un escrito al local ubicado en GETXO, CL AMAIA 22 BJ o mediante correo electrónico, a través de la dirección oicarseleccion@gmail.com

En caso de que el cliente considere que sus datos no se atienden de manera correcta, tiene derecho a presentar una reclamación ante la Agencia Española de Protección de Datos, cuyos datos de contacto son: Teléfonos: 901.100. 099 91.266.35.17; Dirección Postal: C/ Jorge Juan, 6, 28001-Madrid; Sede Electrónica: https://sedeagpd.gob.es/sede-electronica-web/ y página web: www.agpd.es .

☐ Consiento el tratamiento de mis datos de carácter personal con las finalidad de prestar el servicio.

☐ Consiento el tratamiento de mis datos de carácter personal con las finalidad de recibir comunicaciones publicitarias.

Firmado:

*Debe incluirse en la hoja de encargo de los servicios profesionales o en el contrato de prestación de servicios.

** La casilla no puede estar premarcada, siendo obligatoria rellenarla, puesto que sin ella no habría consentimiento para tratar los datos del cliente.

ANEXO VI. FORMULARIO PARA RECOGIDA DE DATOS SENSIBLES

INFORMACIÓN BÁSICA SOBRE PROTECCIÓN DE DATOS

Responsable del tratamiento	ISABEL BUEZO IBAÑEZ Y JOSE ANTONIO GOMEZ SAINZ DE LA MAZA CB CIF: J95720512 Teléfono de contacto: (+34) 944315467 Dirección de contacto principal: Getxo, Cl Amaia 22 Bj Correo electrónico: oicarseleccion@gmail.com
Finalidad del tratamiento	Por lo general, prestación de servicios
Legitimación	Ejecución de un contrato
Derechos	Acceder, rectificar y suprimir los datos, así como otros derechos, como se explica en la información adicional
Procedencia de los datos	Datos obtenidos de los propios clientes No se compran datos a terceros
Información adicional	A continuación, podrá leerla

INFORMACIÓN ADICIONAL

En cumplimiento con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, 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 o RGPD), se comunica que:

- En nombre de la empresa tratamos la información que nos facilita con el fin de prestarles el servicio solicitado y poder ofrecerle productos y servicios de acuerdo con sus intereses. La cesión de sus datos será necesaria para poder prestarles dicho servicio, no pudiendo prestarlo en caso de que no proporcione sus datos.
- Los datos proporcionados se conservarán mientras se mantenga la relación comercial o de prestación de servicios, o durante los años necesarios para cumplir con las obligaciones legales.
- Los datos personales que tratamos proceden del propio interesado o de terceros legitimados para la cesión de los mismos.
- Los datos se cederán, en su caso, a terceras personas, para el cumplimiento de obligaciones legales o con la finalidad de mantener una relación comercial con usted, o en los casos en que fuera imprescindible para la correcta prestación del servicio. En cualquier caso, no se cederán sus datos a terceros países.

- La entidad cumple con el principio de confidencialidad exigido por la normativa vigente y, asimismo, garantiza el cumplimiento de todos los mecanismos de seguridad para la protección de sus datos de carácter personal.
- Usted tiene derecho a obtener confirmación sobre si en nuestra entidad estamos tratando sus datos personales por tanto tiene derecho a solicitar del responsable el acceso a sus datos personales, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos. También tendrá derecho a presentar una reclamación ante la autoridad de control.
- El ejercicio de los derechos se deberá realizar mediante envío de comunicación escrita a la dirección Getxo, Calle Amaia 22 Bk, o bien mediante escrito al correo electrónico oicarseleccion@gmail.com. La solicitud deberá contener el nombre y apellidos del interesado, fotocopia del D.N.I. (o, en su caso, pasaporte o C.I.F.), petición en que se concreta la solicitud, domicilio a efectos de notificaciones, fecha, firma y documentos acreditativos de la petición que se formula. Los modelos se pueden encontrar en https://www.aepd.es/reglamento/derechos/index.html.
- Los datos de carácter personal recogidos por nuestra entidad serán conservados durante el tiempo que sea necesario conforme a la finalidad del tratamiento de los mismos, cumpliendo en todo caso con los plazos legalmente preceptivos exigidos por la normativa aplicable.

☐ Consiento el tratamiento de mis datos de carácter personal con las finalidad de prestar el servicio

☐ Consiento el tratamiento de mis datos de carácter personal con las finalidad de recibir comunicaciones publicitarias.

FECHA

NOMBRE Y APELLIDOS

FIRMA

***¿Cómo ofrecer esta información?

Dos posibilidades:

- En el mismo formulario cumplimentado (por ejemplo, en el reverso)
- Como un anexo o separata que se entregue al interesado

ANEXO VII. ACUSE DE RECIBO DE CV

En primer lugar, le agradecemos el interés que ha mostrado por dirigirse a OICAR SELECCION al enviarnos su currículum vitae.

Le informamos que, de conformidad con la normativa sobre protección de datos, sus datos serán objeto de tratamiento por ISABEL BUEZO IBAÑEZ Y JOSE ANTONIO GOMEZ SAINZ DE LA MAZA CB como responsable del mismo con la finalidad de gestionar su currículum para la selección de personal. Si su perfil no se ajustase a los requisitos buscados en los vigentes procesos de selección procederemos a conservar sus datos para futuros procesos que sí se acomoden a su perfil, salvo que Vd. nos manifestara lo contrario. Su CV será conservado hasta el mes de octubre de cada año independientemente de su llegada.

Contamos con su consentimiento para el tratamiento de los datos que nos ha facilitado, de forma voluntaria, libre e informada al enviarnos su CV al correo electrónico habilitado a tal efecto.

Por otro lado, queremos comunicarle que no cederemos sus datos a terceros, salvo autorización expresa u obligación. Tampoco están previstas transferencias internacionales a terceros países.

Podrá ejercer sus derechos de acceso, rectificación, supresión, oposición, limitación al tratamiento, portabilidad, transparencia en la información y a no ser objeto de decisiones individualizadas automatizadas (incluida la elaboración de perfiles), comunicándolo por escrito, ante esta misma empresa a Getxo, Calle Amaia 22 Bj, o mediante el envío de un correo electrónico a oicarseleccion@gmail.com , adjuntando una fotocopia del DNI o documento similar acreditativo de su identidad.

Sin otro particular, aprovechamos la ocasión para enviarle un cordial saludo.

Atentamente,

XXXX

ANEXO VIII. CONTRATO DE CONFIDENCIALIDAD CON EMPLEADOS

En cumplimiento del 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") le informamos de los siguientes extremos:

Responsable del tratamiento: sus datos pasarán a formar parte de la base de datos de ISABEL BUEZO IBAÑEZ Y JOSE ANTONIO GOMEZ SAINZ DE LA MAZA CB, con domicilio social en Getxo, Cl Amaia 22 Bj.

Finalidad del tratamiento de sus datos:

- El empleado declara que facilita voluntariamente estos datos para el mantenimiento y cumplimiento de la relación, así como para llevar a cabo las gestiones de personal, contable y administrativa de la empresa.
- Recursos humanos: desarrollar, mantener, cumplir y controlar su actividad, y dar cumplimiento a las obligaciones y funciones del departamento de RECURSOS HUMANOS relativas a las actividades de formación, control de asistencia al trabajo, formalización de las nóminas, deberes en materia de prevención de riesgos laborales, así como la gestión de canales de comunicación/denuncias implementadas por la entidad de conformidad con requisitos previstos en las normativas en materia de cumplimientos vigentes.
- Derechos de imagen: utilización de su imagen para la elaboración de publicaciones internas, y para su utilización con finalidades de marketing y

prospección comercial de la entidad, así como a la publicación de su CV e información de su trayectoria profesional en nuestra Intranet, Webs, Redes Sociales y blogs corporativos. En ningún caso estas imágenes e información de carácter personal serán cedidas a terceros, ni utilizadas para una finalidad distinta a la descrita.

Legitimación: se basa en el contrato laboral suscrito con ISABEL BUEZO IBAÑEZ Y JOSE ANTONIO GOMEZ DE LA MAZA CB

Destinatarios: para el cumplimiento de las obligaciones legales, sus datos podrán ser comunicados a:

- Administraciones Públicas (Seguridad Social, Agencia Tributaria, Subvenciones, etc.)
- Mutuas de protección laboral y servicios de prevención de riesgos laborales o la preservación de la salud de los trabajadores.
- Aquellas entidades o clientes que exijan o ante las cuales sea necesario identificar a los empleados: entidades bancarias para el pago de nóminas, aseguradoras, proyectos, formación, mensajería, renting, identificación de infracciones de tráfico, así como aquellas entidades o clientes que requieran datos identificativos y laborales del personal para llevar a cabo el servicio contratado y que acrediten la relación con la empresa.
- Comités de empresa, sindicatos y delegados de prevención.
- Asesoría laboral, si existiese.

Sus datos no serán cedidos para otras finalidades distintas a las descritas.

Derechos. Queda informado de que tiene derecho a obtener confirmación sobre si en ISABEL BUEZO IBAÑEZ Y JOSE ANTONIO GOMEZ DE LA MAZA CB estamos tratando sus datos personales por tanto tiene derecho a solicitar del responsable el acceso a sus datos personales, y su rectificación o supresión, y, en su caso, el derecho a la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos (en cuyo caso únicamente serán conservados para el cumplimiento de las

obligaciones legalmente previstas). También tendrá derecho a presentar una reclamación ante la autoridad de control y a revocar su autorización para el uso de sus imágenes.

El ejercicio de los derechos se deberá realizar dirigiéndose a la siguiente dirección: Getxo, Calle Amaia 22 Bj CB

COMPROMISO DE CONFIDENCIALIDAD

D./Dña. NOMBRE Y APELLIDOS trabajador, con D.N.I. XXXXXX, en el marco de la relación laboral que le une con xxxx empresa, se compromete a:

- No revelar a ninguna persona ajena a OICAR SELECCION, sin el consentimiento debido, información a la que haya tenido acceso en el desarrollo de sus funciones, excepto en aquellos casos en los que sea necesario para dar el debido cumplimiento a sus obligaciones o por habérsele requerido por mandato legal o de la autoridad competente.
- Utilizar la información que se menciona en el apartado anterior únicamente en la forma que exige el desarrollo de sus funciones en OICAR SELECCION y a no utilizarla de otra forma o finalidad.
- No utilizar de ninguna otra manera cualquier información que haya podido obtener utilizando su condición de empleado y que no sea necesaria para el desarrollo de sus funciones.
- Cumplir, en el desarrollo de sus funciones, la normativa vigente relativa a la Protección de Datos de Carácter Personal, y en particular, el RGPD o cualquier otra norma que las sustituya o modifique en el futuro, así como la legislación nacional relativa a protección de datos.
- No utilizar ni incorporar a los sistemas informáticos y archivos documentales de esta entidad la información de carácter personal o empresarial a la que haya tenido acceso durante el desempeño de sus tareas o funciones en otras entidades, cuando ello pueda implicar la vulneración de las legislaciones mencionadas.
- Cumplir los compromisos anteriores aun cuando se extinga, por cualquier causa, la relación laboral que le une a ISABEL BUEZO IBAÑEZ Y JOSE ANTONIO GOMEZ DE LA MAZA CB

- Guardar secreto profesional respecto de los datos personales, datos sobre los clientes, estrategias comerciales y organizativas e industriales, y cualquier otra información a la que tenga acceso con el motivo de las funciones asignadas.
- El empleado declara así mismo conocer que el incumplimiento de este compromiso puede generar el ejercicio de acciones disciplinarias por parte de ISABEL BUEZO IBAÑEZ Y JOSE ANTONIO GOMEZ DE LA MAZA CB, tal como establece el artículo 58 del Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.

De igual modo, le informamos que, con la finalidad de garantizar el derecho a la intimidad y privacidad del trabajador por parte de ISABEL BUEZO IBAÑEZ Y JOSE ANTONIO GOMEZ DE LA MAZA CB, bajo ningún concepto usted debe incorporar a los sistemas informáticos y archivos documentales de esta entidad, su información de carácter personal tales como fotos, vídeos o imágenes.

En el caso de producirse alguna modificación de sus datos, el empleado se compromete a comunicarlo por escrito, con la finalidad de mantener los datos actualizados.

LUGAR Y FECHA

Firma del empleado