DIRECTRICES PARA LA ELABORACIÓN DE CONTRATOS ENTRE RESPONSABLES Y ENCARGADOS DEL TRATAMIENTO

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

apdcat
Autoritat Catalana de Protecció de Dades

Datuak Babesteko Euskal Bulegoa
Agencia Vasca de Protección de Datos

DIRECTRICES PARA LA ELABORACIÓN DE CONTRATOS ENTRE RESPONSABLES Y ENCARGADOS DEL TRATAMIENTO

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

apdcat
Autoritat Catalana de Protecció de Dades

Datuak Babesteko Euskal Bulegoa
Agencia Vasca de Protección de Datos

Indice

El encargado del tratamiento en el Reglamento General de Protección de Datos (RGPD)

Este documento tiene como objetivo identificar los puntos clave a tener presentes en el momento de establecer la relación entre el responsable del tratamiento y el encargado del tratamiento, así como identificar las cuestiones que afectan de forma directa a la gestión de la relación entre ambos.

Asimismo pretende ofrecer orientaciones, a modo de recomendación, para confeccionar el documento que regule dicha relación.

1.- ¿Qué es un encargado del tratamiento y cuál es su función principal?

El encargado del tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que presta un servicio al responsable que conlleva el tratamiento de datos personales por cuenta de éste.

Los tipos de encargado del tratamiento y las formas en que se regulará su relación pueden ser tan variados como los tipos de servicios que puedan suponer acceso a datos personales. Así, podemos encontrar servicios cuyo objeto principal es el tratamiento de datos personales (por ejemplo, una empresa o entidad pública que ofrece un servicio de alojamiento de información en sus servidores) y otros que tratan datos personales sólo como consecuencia de la actividad que presta por cuenta del responsable del tratamiento (por ejemplo el gestor de un servicio público municipal).

Pese a que la definición puede parecer clara, en la práctica se dan multitud de situaciones donde puede ser difícil deslindar cuándo estamos frente a un encargado o a un responsable del tratamiento. Para facilitar esta distinción, debemos tener en cuenta que corresponde al responsable decidir sobre la finalidad y los usos de la información, mientras que el encargado del tratamiento debe cumplir con las instrucciones de quien le encomienda un determinado servicio, respecto al correcto tratamiento de los datos personales a los que pueda tener acceso como consecuencia de la prestación de este servicio.

Cuando sea de aplicación el texto Refundido de la Ley de Contratos del Sector Público, aprobado por el Real Decreto Legislativo 3/2011, de 14 de noviembre, debe tenerse en cuenta que dicha ley prevé (disposición adicional 26ª) que, cuando la contratación implique el acceso del contratista a datos de carácter personal de cuyo tratamiento sea responsable la entidad contratante, el contratista tendrá la consideración de encargado del tratamiento. En estos casos también será de aplicación el régimen establecido en el RGPD.

2.- ¿Qué tratamientos puede llevar a cabo un encargado sobre los datos que le han sido encomendados?

El encargado puede realizar todos los tratamientos, automatizados o no, que el responsable del tratamiento le haya encomendado formalmente. La definición de tratamiento nos permite concretarlos atendiendo al ciclo de vida de la información: recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

En todo caso, deben quedar claramente delimitados en el acuerdo que se adopte.

3.- ¿Qué nivel de decisión puede asumir un encargado del tratamiento?

El encargado del tratamiento puede adoptar todas las decisiones organizativas y operacionales necesarias para la prestación del servicio que tenga contratado. En ningún caso puede variar las finalidades y los usos de los datos ni los puede utilizar para sus propias finalidades.

Las decisiones que adopte deben respetar en todo caso las instrucciones dadas por el responsable del tratamiento.

4.- ¿Puede el responsable del tratamiento elegir cualquier encargado del tratamiento?

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

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

Para demostrar que el encargado ofrece garantías suficientes, el RGPD prevé que la adhesión a códigos de conducta o la posesión de un certificado de protección de datos pueden servir como mecanismos de prueba.

5.- ¿Cómo deben regularse las relaciones entre el responsable y el encargado del tratamiento?

La regulación de la relación entre el responsable y el encargado del tratamiento debe establecerse a través de un contrato o de un acto jurídico similar que los vincule. El contrato o acto jurídico debe constar por escrito, inclusive en formato electrónico.

La posibilidad de regular esta relación a través de un acto jurídico unilateral del responsable del tratamiento es una de las novedades previstas en el RGPD. En cualquier caso debe tratarse de un acto jurídico que establezca y defina la posición del encargado del tratamiento, siempre y cuando ese acto vincule jurídicamente al encargado del tratamiento. Este sería el caso, por ejemplo, de una resolución administrativa que conste notificada al encargado del tratamiento.

En cualquier caso, ya se trate de un acuerdo o de otro acto jurídico, su contenido debe reunir los requisitos establecidos en el RGPD, a los que más adelante se hace referencia.

El contenido del acto o acuerdo puede basarse en cláusulas tipo establecidas por la Comisión Europea o por la autoridad de control, inclusive cuando formen parte de una certificación otorgada al responsable o al encargado del tratamiento.

Los modelos de cláusulas que se incluyen en el Anexo 1 de este documento no tienen la consideración de cláusulas tipo a los efectos del artículo 28.8 del RGPD, sino que son simplemente un modelo orientativo para que los diferentes responsables puedan adaptarlo a las necesidades derivadas de su propia organización.

6.- ¿Quién es responsable de los tratamientos realizados por el encargado?

El responsable del tratamiento no pierde esta consideración en ningún caso y, por tanto, continúa siendo responsable del correcto tratamiento de los datos personales y de la garantía de los derechos de las personas afectadas. El responsable tiene una obligación de especial diligencia en la elección y supervisión del encargado.

7.- ¿El RGPD se aplica sólo a los encargados establecidos en el territorio de la Unión Europea?

No, el Reglamento se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no.

Por otra parte, el RGPD también se aplicará al tratamiento de datos personales de interesados que residan en la Unión realizado por un encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con:

a) La oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si se les requiere su pago.

b) El control de su comportamiento, en la medida en que tenga lugar en la Unión.

8.- ¿Existe un régimen especial para la contratación de un encargado que no esté establecido en el territorio de la Unión Europea o que efectúe el tratamiento fuera del territorio de la Unión?

La comunicación de datos personales, en el marco de un acuerdo de encargado del tratamiento, a un país que no forme parte de la Unión se rige por la regulación establecida en el Reglamento para las transferencias internacionales.

La transferencia a un tercer país en ningún caso puede suponer una reducción del nivel de protección de las personas que establece el Reglamento. Este principio también se aplica en las transferencias posteriores de datos personales, desde el tercer país a otro tercer país o una organización internacional.

Para la transferencia de datos a países que no garantizan un nivel de protección adecuado, el responsable deberá acreditar que el encargado del tratamiento está en disposición de ofrecer garantías adecuadas y, en todo caso, garantizar que los interesados cuenten con derechos exigibles y acciones legales efectivas.

9.- ¿Si se externaliza las funciones del delegado de protección de datos a un tercero, éste tiene la consideración de encargado del tratamiento?

Sí, el RGPD prevé que el delegado de protección de datos debe poder acceder a los datos que se traten. Por tanto, deberá formalizarse un encargo del tratamiento.

10.- ¿Es necesario informar a los interesados de la contratación de un encargado del tratamiento?

El RGPD no establece la obligación de informar respecto a la contratación de un encargado del tratamiento. Pese a esto, en determinadas circunstancias (atendiendo, por ejemplo, a la naturaleza del tratamiento o de los datos tratados, o por otras circunstancias concurrentes) puede ser aconsejable dar esta información para una mayor transparencia en el tratamiento de los datos personales.

11.- ¿Cuál es el contenido mínimo de un acuerdo o acto de encargo del tratamiento?

Como mínimo debe establecerse el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable.

En particular, el acuerdo o acto debe contener:

A.- LAS INSTRUCCIONES DEL RESPONSABLE DEL TRATAMIENTO

Se debe documentar de forma precisa las instrucciones respecto del encargo realizado. Es necesario identificar de forma clara y concreta cuáles son los tratamientos de datos a realizar por el encargado del tratamiento, atendiendo al tipo de servicio prestado y a la forma de prestarlo. Es especialmente necesario determinar de forma clara las comunicaciones a terceros que el responsable encomienda al encargado o que se derivan del servicio prestado.

La sujeción a las instrucciones del responsable deberá producirse igualmente en el caso de las transferencias internacionales de datos que puedan producirse como consecuencia de la prestación del servicio. Si el encargado del tratamiento está obligado legalmente, por el Derecho de la Unión o de un Estado miembro, a transferir datos a un tercer país deberá informar al responsable antes de llevar a cabo el tratamiento, salvo que tal derecho lo prohíba por razones importantes de interés público.

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 deberá informar inmediatamente al responsable.

B.- EL DEBER DE CONFIDENCIALIDAD

Hay que establecer la forma en que el encargado del tratamiento garantizará que las personas autorizadas para tratar datos personales se han comprometido, de forma expresa, a respetar la confidencialidad o, en su caso, si están sujetas a una obligación de confidencialidad de naturaleza estatutaria.

El cumplimiento de esta obligación debe quedar documentado y a disposición del responsable del tratamiento.

C.- LAS MEDIDAS DE SEGURIDAD

El acuerdo debe establecer la obligación del encargado de adoptar todas las medidas de seguridad necesarias, de conformidad con lo establecido en el artículo 32 del RGPD.

Corresponde al responsable del tratamiento realizar la evaluación de riesgos para determinar las medidas de seguridad apropiadas para garantizar la seguridad de la información tratada y los derechos de las personas afectadas. Así mismo el encargado también debe evaluar los posibles riesgos derivados del tratamiento, teniendo en cuenta los medios utilizados (tecnologías, recursos etc.) y otras circunstancias que puedan incidir en la seguridad, como por ejemplo que el encargado lleve a cabo otros tratamientos.

A partir de aquí, la determinación de las medidas de seguridad concretas puede realizarse a través de una lista exhaustiva de las mismas o de la remisión a un estándar o marco nacional o internacional reconocido.

Así, teniendo en cuenta el estado de la técnica, los costes de aplicación y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y las libertades de las personas físicas, el responsable y el encargado del tratamiento establecerán las medidas técnicas y organizativas apropiadas para garantizar el nivel de seguridad adecuado al riesgo existente que, en su caso, incluyan, entre otros:

a) La seudoanimización 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) Un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

La adhesión a códigos de conducta o la posesión de una certificación son elementos que sirven para demostrar el cumplimiento de los requisitos anteriormente indicados.

El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo su autoridad y tenga acceso a datos personales sólo pueda tratarlos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros.

D.- EL RÉGIMEN DE LA SUBCONTRATACIÓN

El acuerdo debe establecer el régimen de subcontratación. El RGPD exige la autorización previa por escrito del responsable del tratamiento para que el encargado del tratamiento pueda recurrir a otro encargado (subencargado) para desarrollar el servicio encomendado, cuando esto conlleve el tratamiento de los datos personales por parte de un tercero.

Esta autorización puede ser específica (identificación de la entidad concreta) o general (sólo autorizando la subcontratación, pero sin concretar la entidad).

En el supuesto que la autorización sea de carácter general, el encargado informará al responsable de la incorporación de un subencargado o su sustitución por otros subencargados, dando así al responsable la oportunidad de oponerse a dichos cambios.

Puede ser de utilidad establecer en el acuerdo o acto la forma (que en todo caso deberá constar por escrito) y el plazo para que el responsable pueda manifestar su oposición.

En todo caso, el subencargado del tratamiento debe estar sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad…) y en la misma forma (acuerdo por escrito o acto jurídico vinculante) que el encargado del tratamiento en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas. En caso de incumplimiento por el subencargado, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento en lo referente al cumplimiento de las obligaciones del subencargado.

Cuando sea aplicable la legislación de contratos del sector público, habrá que tener en cuenta también las disposiciones específicas previstas en dicha ley.

E.- LOS DERECHOS DE LOS INTERESADOS

Hay que establecer la forma en la que el encargado del tratamiento asistirá al responsable en el cumplimento de la obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III del RGPD:

- Acceso a datos personales
- Rectificación
- Supresión (derecho al olvido)
- Limitación del tratamiento
- Portabilidad de datos
- Oposición
- A no ser objeto de decisiones individualizadas automatizadas (incluida la elaboración de perfiles)

El acuerdo deberá establecer de forma clara si corresponde al encargado del tratamiento atender y dar respuesta a las solicitudes de estos derechos o bien establecer expresamente

que su única obligación es comunicar al responsable del tratamiento que se ha ejercido un derecho.

En el primer supuesto, el acuerdo debe establecer la forma y los plazos para atender o, en su caso, dar respuesta a las solicitudes de ejercicio de derechos. En el segundo supuesto, debe establecerse la forma y el plazo en que la solicitud y, en su caso, la información correspondiente al ejercicio del derecho se debe comunicar al responsable del tratamiento.

En cuanto al derecho de información de las personas afectadas, se trata de un derecho no sujeto a solicitud y, por tanto, no sujeto a las previsiones del artículo 28.3.e) del RGPD. Pese a ello, en aquellos casos en que el encargado deba realizar la recogida de datos es recomendable establecer en el acuerdo o acto jurídico la forma y el momento en que debe darse el derecho de información.

F.- La colaboración en el cumplimiento de las obligaciones del responsable

Se debe establecer la forma en que el encargado ayudará al responsable a garantizar el cumplimiento de las obligaciones relativas a la aplicación de las medidas de seguridad que correspondan, la notificación de violaciones de datos a las Autoridades de Protección de Datos, la comunicación de violaciones de datos a los interesados, la realización de las evaluaciones de impacto relativa la protección de datos y, en su caso, la realización de consultas previas.

El cumplimiento de esta obligación queda supeditado a la naturaleza del tratamiento realizado y a la información que esté a disposición del encargado.

El responsable puede delegar en el encargado el cumplimiento de estas obligaciones.

G.- El destino de los datos al finalizar la prestación

Hay que prever si, una vez finalice la prestación de los servicios de tratamiento, el encargado del tratamiento debe proceder a la supresión o a la devolución de los datos personales y de cualquier copia existente, ya sea al responsable o a otro encargado designado por el responsable.

El acuerdo debe establecer de forma clara cuál de las dos opciones es la elegida por el responsable, así como la forma y el plazo en que debe cumplirse.

En todo caso, los datos deberán ser devueltos al responsable cuando se requiera la conservación de los datos personales, en virtud del Derecho de la Unión o de los Estados miembros.

No obstante, el encargado puede conservar una copia con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

H.- LA COLABORACIÓN CON EL RESPONSABLE PARA DEMOSTRAR EL CUMPLIMIENTO

Es preciso establecer la obligación del encargado de poner a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, realizadas por el responsable o por otro auditor autorizado por el responsable.

ANEXO I

Ejemplo de cláusulas contractuales para supuestos en que el encargado del tratamiento trate los datos en sus locales y exclusivamente con sus sistemas

(Estas cláusulas tienen sólo carácter orientativo y deben adaptarse a las circunstancias concretas del tratamiento que se lleve a cabo)

1. Objeto del encargo del tratamiento

Mediante las presentes cláusulas se habilita a la entidad ....., encargada del tratamiento, para tratar por cuenta de ...., responsable del tratamiento, los datos de carácter personal necesarios para prestar el servicio de ....

El tratamiento consistirá en: *(descripción detallada del servicio)*

Concreción de los tratamientos a realizar:

☐ Recogida	☐ Registro
☐ Estructuración	☐ Modificación
☐ Conservación	☐ Extracción
☐ Consulta	☐ Comunicación por transmisión
☐ Difusión	☐ Interconexión
☐ Cotejo	☐ Limitación
☐ Supresión	☐ Destrucción
☐ Conservación	☐ Comunicación

☐ Otros:.....

2. Identificación de la información afectada

Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, la *entidad/órgano*....., responsable del tratamiento, pone a disposición de la entidad ....., encargada del tratamiento, la información que se describe a continuación:

- ……
- ……

3. Duración

El presente acuerdo tiene una duración de .....[1]

Una vez finalice el presente contrato, el encargado del tratamiento debe *suprimir/devolver al responsable/devolver a otro encargado que designe el responsable (indicar la opción que proceda)* los datos personales y suprimir cualquier copia que esté en su poder.

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[2] de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable, que contenga:

   1. El nombre y los datos de contacto del encargado o encargados 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.
   2. Las categorías de tratamientos efectuados por cuenta de cada responsable.
   3. 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.
   4. Una descripción general de las medidas técnicas y organizativas de seguridad relativas a:

      a) La seudoanimización 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.

[1] En algunos casos, en particular determinados casos sometidos al derecho administrativo (convenios, contratos de gestión de servicios públicos, etc.), la duración del encargo puede estar limitada por la duración establecida por la legislación vigente para la prestación de servicios.

[2] Las obligaciones indicadas en los apartados 1 y 2 no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, salvo que el tratamiento que realice pueda suponer un riesgo para los derechos y las libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1 del RGPD, o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10 de dicho Reglamento.

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. Subcontratación

   (Escoger una de las opciones)

   Opción A — *No subcontratar ninguna de las prestaciones que formen parte del objeto de este contrato que comporten el tratamiento de datos personales, salvo los servicios auxiliares necesarios para el normal funcionamiento de los servicios del encargado.*

   Si fuera necesario subcontratar algún tratamiento, este hecho se deberá comunicar previamente y por escrito al responsable, con una antelación de .....[3], 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.

   Opción B — *Se autoriza al encargado a subcontratar con la empresa …..... las prestaciones que comporten los tratamientos siguientes:*
   .....

[3] Se recomienda establecer un plazo mínimo de antelación para realizar la comunicación.

Para subcontratar con otras empresas, el encargado debe comunicarlo por escrito al responsable, 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 de ……[4].

El subcontratista, que también tiene 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[5] 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. Asistir al responsable del tratamiento en la respuesta al ejercicio de los derechos de:

1. Acceso, rectificación, supresión y oposición
2. Limitación del tratamiento
3. Portabilidad de datos
4. A no ser objeto de decisiones individualizadas automatizadas (incluida la elaboración de perfiles)

(Escoger una de las opciones)

Opción A *El encargado del tratamiento debe resolver, por cuenta del responsable, y dentro del plazo establecido, las solicitudes de ejercicio de los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones individualizadas automatizadas, en relación con los datos objeto del encargo.[6]*

[4] Se recomienda establecer un plazo mínimo de antelación para realizar la comunicación.

[5] Si existe una obligación de confidencialidad de naturaleza estatutaria deberá quedar constància expresa de la naturaleza y extensión de esta obligación.

[6] A pesar de que la delegación en el encargado es una decisión que corresponde al responsable, resulta especialmente recomendable en aquellos supuestos en que los datos se traten exclusivamente con los sistemas del encargado.

Opción B *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 del tratamiento, éste debe comunicarlo por correo electrónico a la dirección ……. (dirección que indique el responsable). La comunicación debe hacerse de forma inmediata y en ningún caso más allá del día laborable siguiente al de la recepción de la solicitud[7], juntamente, en su caso, con otras informaciones que puedan ser relevantes para resolver la solicitud.*

k. Derecho de información

(Escoger una de las opciones)

Opción A *El encargado del tratamiento, en el momento de la recogida de los datos, debe facilitar la información relativa a los tratamientos de datos que se van a realizar. La redacción y el formato en que se facilitará la información se debe consensuar con el responsable antes del inicio de la recogida de los datos.*

Opción B *Corresponde al responsable 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 máximo de ……..[8], y a través de…… , 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.

[7] Plazo y medio recomendados a fin de que el responsable pueda resolver la solicitud dentro del plazo establecido.
[8] El plazo debe ser inferior a 72 horas en cualquier caso.

(Escoger alguna o las dos opciones)[9]

Opción A

Corresponde al encargado del 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.

Opción B

Corresponde al encargado del tratamiento comunicar en el menor tiempo posible las violaciones de la seguridad de los datos a los interesados, cuando sea probable que la violación suponga un alto riesgo para los derechos y las libertades de las personas físicas.

La comunicación debe realizarse en un lenguaje claro y sencillo y deberá, como mínimo:

a) Explicar la naturaleza de la violación de datos.
b) Indicar 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) Describir las posibles consecuencias de la violación de la seguridad de los datos personales.
d) Describir las medidas adoptadas o propuestas por el responsable del tratamiento 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.

[9] Pese a que la notificación de las violaciones de seguridad a la autoridad de control o a los interesados corresponde al responsable del tratamiento, en aquellos supuestos en que los datos se traten exclusivamente con los sistemas del encargado puede ser recomendable atribuir dichas funciones al encargado.

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 siguientes:

(Escoger una o las dos opciones)

Opción A Las medidas de seguridad siguientes, de acuerdo con la evaluación de riesgos realizada por[10]…… , en fecha …… :

- *……*
- *……*
- *……*

Opción B Las medidas de seguridad establecidas en[11] ....

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. Designar un delegado de protección de datos[12] y comunicar su identidad y datos de contacto al responsable.

r. Destino de los datos

(Escoger una de las tres opciones)

[10] Indicar si la evaluación de riesgos ha sido realizada por el responsable o por el encargado del tratamiento.
[11] Indicar el código de conducta, el sello, la certificación u otro estándar donde están definidas las medidas aplicables.
[12] El delegado de protección de datos debe designarse cuando:
a) El tratamiento lo lleve a cabo una autoridad o un organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;
b) Las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala;
c) Las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales y de datos relativos a condenas e infracciones penales.

Opción A

Devolver al responsable del tratamiento los datos de carácter personal y, si procede, los soportes donde consten, una vez cumplida la prestación.

La devolución debe comportar el borrado total de los datos existentes en los equipos informáticos utilizados por el encargado.

No obstante, el encargado puede conservar una copia, con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

Opción B

Devolver al encargado que designe por escrito el responsable del tratamiento, los datos de carácter personal y, si procede, los soportes donde consten, una vez cumplida prestación.

La devolución debe comportar el borrado total de los datos existentes en los equipos informáticos utilizados por el encargado.

No obstante, el encargado puede conservar una copia, con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

Opción C

Destruir los datos, una vez cumplida la prestación. Una vez destruidos, el encargado debe certificar su destrucción por escrito y debe entregar el certificado al responsable del tratamiento.

No obstante, el encargado puede conservar una copia, con los datos debidamente boqueados, 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 documento.

b) Realizar una evaluación del impacto en la protección de datos personales de las operaciones de tratamiento a realizar por el encargado.

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.


AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS


apdcat
Autoritat Catalana de Protecció de Dades


Datuak Babesteko
Euskal Bulegoa
Agencia Vasca de
Protección de Datos