

GUÍA PARA EL CUMPLIMIENTO DEL DEBER DE INFORMAR

AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS



apdcat
Autoritat Catalana de Protecció de Dades



Datuak Babesteko
Euskal Bulegoa
Agencia Vasca de
Protección de Datos

GUÍA PARA EL CUMPLIMIENTO DEL DEBER DE INFORMAR

AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS



apdcat
Autoritat Catalana de Protecció de Dades



Datuak Babesteko
Euskal Bulegoa
Agencia Vasca de
Protección de Datos

Índice

1	¿A quién va dirigida esta guía?	2
2	¿Qué cambia el RGPD sobre el deber de informar?.....	2
3	¿Quién y cuándo debe informar?	3
4	¿Dónde y cómo informar?	4
5	Información por capas	5
6	Información básica (primera capa)	6
7	Información adicional (segunda capa)	8
7.1	Epígrafe “Responsable”	9
7.2	Epígrafe “Finalidad”	10
7.3	Epígrafe “Legitimación”	11
7.4	Epígrafe “Destinatarios”	13
7.5	Epígrafe “Derechos”	14
7.6	Epígrafe “Procedencia”	15

1 ¿A quién va dirigida esta guía?

- El Reglamento General de Protección de Datos¹ (en adelante, RGPD), publicado en mayo de 2016 y aplicable a partir del 25 de mayo de 2018, es una norma de aplicación directa en toda la Unión Europea, 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. El RGPD sustituirá, a partir de mayo de 2018, a la actual Ley Orgánica de Protección de Datos² (en adelante, LOPD) y al Reglamento RD-1720/2007, que la desarrolla, e introduce una serie de cambios y novedades a los cuales es necesario adaptar los actuales tratamientos, con anterioridad a la fecha de su plena aplicación.
- El objeto de esta Guía, de forma específica, es **orientar acerca de las mejores prácticas para dar cumplimiento a la obligación de informar a los interesados**, en virtud del principio de transparencia, acerca de las circunstancias y condiciones del tratamiento de datos a efectuar, así como de los derechos que les asisten. Esta guía cubre únicamente este objetivo específico, y debe ser complementada con otras guías que las Autoridades de Protección de Datos puedan emitir, en relación con la aplicación del RGPD.
- La Guía va dirigida, en primer lugar, a los Responsables³ de Tratamientos a quienes resulte aplicable el RGPD, así como a los profesionales que contribuyen, ya sea dentro de sus Organizaciones o bien como Encargados⁴ de Tratamiento, a las tareas de asesorar a los Responsables de Tratamientos, respecto de las obligaciones que les incumben en virtud del Reglamento.
- En especial, la guía también está dirigida a quienes desempeñen o vayan a desempeñar el rol de Delegado⁵ de Protección de Datos (en adelante, DPD), figura novedosa en nuestro ámbito, a la que el RGPD otorga un destacado papel.

2 ¿Qué cambia el RGPD sobre el deber de informar?

- **Actualmente**, la **LOPD** establece las siguientes obligaciones respecto de la información que se ha de facilitar a las personas interesadas en el momento en que se soliciten los datos:
 - ✓ La existencia del fichero o tratamiento, su finalidad y destinatarios.

¹ B.O.E.: <https://www.boe.es/doue/2016/119/L00001-00088.pdf>

² B.O.E.: <https://www.boe.es/buscar/pdf/1999/BOE-A-1999-23750-consolidado.pdf>

³ «Responsable»: “persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, **determine los fines y medios del tratamiento**”

⁴ «Encargado»: “persona física o jurídica, autoridad pública, servicio u otro organismo que **trate datos personales por cuenta del responsable** del tratamiento”

⁵ «Delegado de Protección de Datos»: “persona física o jurídica, empleado en plantilla o mediante contrato de servicio, que informa y asesora al Responsable, al Encargado y a otros empleados sobre las obligaciones del RGPD y supervisa su cumplimiento, cooperando y actuando como punto de contacto con las Autoridades de Control”

- ✓ El carácter obligatorio o no de la respuesta, así como de sus consecuencias.
 - ✓ La posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
 - ✓ La identidad y datos de contacto del responsable del tratamiento.
- **A partir de ahora**, el **RGPD** añade **requisitos adicionales** en cuanto a la necesidad de informar a las personas interesadas, generalizando el concepto de “Tratamiento”⁶, e incorporando, en líneas generales, los siguientes detalles:
 - ✓ Los datos de contacto del Delegado de Protección de Datos, en su caso,
 - ✓ La base jurídica o legitimación para el tratamiento,
 - ✓ El plazo o los criterios de conservación de la información,
 - ✓ La existencia de decisiones automatizadas o elaboración de perfiles,
 - ✓ La previsión de transferencias a Terceros Países
 - ✓ El derecho a presentar una reclamación ante las Autoridades de Control

Y además, en el caso de que los datos no se obtengan del propio interesado:

- ✓ El origen de los datos
 - ✓ Las categorías de los datos
- En consecuencia, los procedimientos, modelos o formularios diseñados de conformidad con la LOPD **deberán ser revisados y adaptados** por los Responsables de Tratamientos **con anterioridad a la fecha de plena aplicación** del RGPD, incorporando los nuevos requisitos de acuerdo con las directrices que se proporcionan en esta guía.
Puesto que los nuevos requisitos amplían y no contradicen la obligación de informar establecida en la LOPD, se recomienda revisar y aplicar dicha adaptación **cuanto antes**.
 - Para mayor detalle pueden consultarse los artículos 13 y 14 del RGPD, relativos al derecho de información de las personas interesadas.

3 ¿Quién y cuándo debe informar?

- La obligación de informar a las personas interesadas sobre las circunstancias relativas al tratamiento de sus datos **recae sobre el Responsable** del Tratamiento.
- La información se debe poner a disposición de los interesados **en el momento en que se soliciten los datos**, previamente a la **recogida o registro**, si es que los datos se obtienen directamente del interesado.
- En el caso de que los datos no se obtengan del propio interesado, por proceder de alguna cesión legítima, o de fuentes de acceso público, el Responsable informará a las personas interesadas **dentro de un plazo razonable**, pero en cualquier caso:
 - ✓ antes de un mes desde que se obtuvieron los datos personales,
 - ✓ antes o en la primera comunicación con el interesado,

⁶ «Tratamiento»: “cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la 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” (el RGPD no hace uso del concepto de “fichero”)

- ✓ antes de que los datos, en su caso, se hayan comunicado a otros destinatarios
- Esta obligación se debe cumplir **sin necesidad de requerimiento** alguno, y el responsable deberá **poder acreditar** con posterioridad que la obligación de informar ha sido satisfecha.

¿Cuándo NO es preciso informar?

- Únicamente no será necesario informar **cuando el interesado ya disponga de la información**, ni tampoco, en el caso de que los datos no procedan del interesado, cuando:
 - ✓ la comunicación resulte imposible o suponga un esfuerzo desproporcionado,
 - ✓ el registro o la comunicación esté expresamente establecido por el Derecho de la Unión o de los Estados miembros,
 - ✓ cuando los datos deban seguir teniendo carácter confidencial por un deber legal de secreto.

4 ¿Dónde y cómo informar?

- Los procedimientos de recogida de información pueden ser muy variados y, en consecuencia, los modos de informar a las personas interesadas deben adaptarse a las circunstancias de cada uno de los medios empleados para la recopilación o registro de los datos. Por ejemplo, algunas de las formas más habituales de recogida de datos y, en consecuencia, a través de los cuales hay que informar, pueden ser:

- | | |
|---------------------------------|------------------------------------|
| ✓ Formularios en papel, | ✓ Entrevista telefónica |
| ✓ Navegación o formularios Web, | ✓ Registro de aplicaciones móviles |
| ✓ Datos de actividad personal | ✓ Datos de sensores (IoT) |
| | ✓ |

- Por otra parte, las comunicaciones al interesado sobre datos ya disponibles, o tratamientos adicionales, pueden hacerse llegar, entre otros, por medio de:

- | | |
|---|--------------------------|
| ✓ Correo postal | ✓ Mensajería electrónica |
| ✓ Notificaciones emergentes en servicios y aplicaciones | |

- Las características de cada uno de los medios varían en cuanto a extensión, disponibilidad de espacio, legibilidad, posibilidad de vincular informaciones, etc. En cualquier caso, la información a las personas interesadas debe proporcionarse:

- ✓ con un lenguaje **claro y sencillo**,
- ✓ de forma **concisa, transparente, inteligible y de fácil acceso**.

5 Información por capas

- Para hacer compatible la mayor exigencia de información que introduce el RGPD y la concisión y comprensión en la forma de presentarla, desde las Autoridades de Protección de Datos se recomienda adoptar un modelo de **información por capas o niveles**.
- El enfoque de información multinivel consiste en lo siguiente:
 - ✓ presentar una **información básica** en un primer nivel, de forma **resumida**, en el mismo momento y en el mismo medio en que se recojan los datos,
 - ✓ remitir a la **información adicional** en un segundo nivel, donde se presentarán **detalladamente** el resto de las informaciones, en un medio más adecuado para su presentación, comprensión y, si se desea, archivo.
- El conjunto de las informaciones requeridas por el RGPD pueden agruparse en unos determinados **epígrafes**, a los efectos de su organización y presentación, especialmente en cuanto a la información a presentar, de forma resumida, en la primera capa o nivel.

Por ejemplo, una agrupación recomendada, junto con el resumen de la información a presentar en cada capa o nivel, puede ser la siguiente:

Epígrafe	Información básica (1ª capa, resumida)	Información adicional (2ª capa, detallada)
“ Responsable ” (del tratamiento)	Identidad del Responsable del Tratamiento	Datos de contacto del Responsable
		Identidad y datos de contacto del representante
		Datos de contacto del Delegado de Protección de Datos
“ Finalidad ” (del tratamiento)	Descripción sencilla de los fines del tratamiento, incluso elaboración de perfiles	Descripción ampliada de los fines del tratamiento
		Plazos o criterios de conservación de los datos
		Decisiones automatizadas, perfiles y lógica aplicada
“ Legitimación ” (del tratamiento)	Base jurídica del tratamiento	Detalle de la base jurídica del tratamiento, en los casos de obligación legal, interés público o interés legítimo.
		Obligación o no de facilitar datos y consecuencias de no hacerlo
“ Destinatarios ” (de cesiones o transferencias)	Previsión o no de Cesiones	Destinatarios o categorías de destinatarios
	Previsión de Transferencias, o no, a terceros países	Decisiones de adecuación, garantías, normas corporativas vinculantes o situaciones específicas aplicables
“ Derechos ” (de las personas interesadas)	Referencia al ejercicio de derechos.	Cómo ejercer los derechos de acceso, rectificación, supresión y portabilidad de sus datos, y la limitación u oposición a su tratamiento
		Derecho a retirar el consentimiento prestado
		Derecho a reclamar ante la Autoridad de Control
“ Procedencia ” (de los datos)	Fuente de los datos (cuando no proceden del interesado)	Información detallada del origen de los datos, incluso si proceden de fuentes de acceso público
		Categorías de datos que se traten

- Se recomienda **presentar siempre** los cinco primeros epígrafes (“*Responsable*”, “*Finalidad*”, “*Legitimación*”, “*Destinatarios*” y “*Derechos*”), añadiendo el epígrafe “*Procedencia*” únicamente cuando los datos no procedan del propio interesado.
- Es importante destacar que este enfoque multinivel se introduce con la finalidad, por un lado, de **facilitar la tarea del Responsable** del Tratamiento a la hora de diseñar sus procedimientos y formularios, y por otro, de conseguir que las personas interesadas obtengan la información más relevante **de forma rápida y simplificada**, pero sin que ello suponga **ningún menoscabo** de los principios de **licitud, lealtad y transparencia** que establece el RGPD.

6 Información básica (primera capa)

- La forma de presentación preferente de esta primera capa es **en forma de tabla** (de manera análoga a como se presenta la información nutricional alimentaria), garantizando que dicha información quede dentro del “campo de visión” del interesado, según sea el medio utilizado en la recogida de la información.
- Debe estar claramente identificada con un título tal como “**Información básica sobre protección de datos**”
 - ✓ Por ejemplo, en un formulario de solicitud, la tabla con la información básica debería situarse en el mismo campo de visión que el lugar donde haya de manifestarse la conformidad con lo solicitado (la firma, si es en papel, o el botón de “enviar”, si es un formulario electrónico), formando parte de la copia que quede a disposición del interesado.
 - ✓ Si, por restricciones del diseño, no fuese factible, debe incorporarse una nota o llamada en el campo de visión de la firma, informando sobre dónde se sitúa la tabla con la información sobre protección de datos.

▪ Ejemplo: “*antes de firmar la solicitud, debe leer la información básica sobre protección de datos que se presenta en (...el reverso, al pié, etc...)*”

- El epígrafe de “**Legitimación**” hace referencia a la base jurídica en la que se basa el tratamiento, la cual viene regulada en el RGPD⁷, con las siguientes posibilidades⁸:
 - ✓ “Ejecución de un contrato”
 - ✓ “Cumplimiento de una obligación legal”
 - ✓ “Misión en Interés público” o “Ejercicio de Poderes Públicos”
 - ✓ “Interés legítimo del Responsable” o “Interés legítimo de un tercero”
 - ✓ “Consentimiento del interesado”

Cuando un tratamiento persiga varias finalidades se hará constar aquí la legitimación para la **finalidad principal** del tratamiento.

- El epígrafe de “**Destinatarios**” debe aparecer siempre en la información básica, aun cuando no se haya previsto comunicar los datos a terceros, puesto que ello contribuye a facilitar a los interesados una mejor comprensión del tratamiento.

⁷ Para mayor detalle, véase el artículo 6 RGPD sobre la licitud del tratamiento

⁸ No se incluye aquí la legitimación por “protección de intereses vitales” del interesado o de otra persona. Para mayor información, véase más adelante, en el epígrafe correspondiente, dentro de la información adicional.

▪ Ejemplo: “No se cederán datos a terceros, salvo obligación legal”

- El epígrafe “**Derechos**” también debe aparecer siempre en la información básica, si bien puede hacerse una breve alusión a la existencia de los derechos más habituales y una referencia al correspondiente epígrafe en la información adicional.

▪ Ejemplo: “Tiene derecho a acceder, rectificar y suprimir los datos, así como otros derechos, como se explica en la información adicional”

- Finalmente, además de la tabla con la información resumida, debe incluirse claramente una indicación sobre **dónde o cómo puede accederse** a la información adicional en la segunda capa.

▪ Ejemplo: “Puede consultar la información adicional y detallada sobre Protección de Datos en (...indicación textual, hipervínculo, etc...)”

Ejemplo de Información básica en papel

- Un caso trivial de información resumida, presentada en forma de tabla, utilizada en un formulario en papel para, por ejemplo, la suscripción a una revista podría ser el siguiente:

Información básica sobre Protección de Datos	
Responsable	Ediciones Warren&Brandeis, S.A.
Finalidad	Gestión de la suscripción
Legitimación	Ejecución de un contrato
Destinatarios	No se cederán datos a terceros, salvo obligación legal
Derechos	Acceder, rectificar y suprimir los datos, así como otros derechos, como se explica en la información adicional
Información adicional	Puede consultar la información adicional y detallada sobre Protección de Datos en nuestra página web: http://www.warrenbrandeis.com/protecciondatos

- Obsérvese que, aunque se trata de un formulario en soporte papel, se ha incluido la referencia a la información adicional en forma de hipervínculo, por asumir que se trata de un supuesto con limitación material de espacio.

Ejemplo de Información básica en un medio electrónico

- Un caso de información resumida, utilizada en un formulario web para, por ejemplo, solicitar la descarga de cierta documentación, que implica darse de alta en una lista de distribución de información comercial, podría ser el siguiente:

Información básica sobre Protección de Datos	
Responsable	Ediciones Warren&Brandeis, S.A. +info...
Finalidad	Gestionar el envío de información y prospección comercial +info...
Legitimación	Consentimiento del interesado +info...
Destinatarios	Otras empresas del grupo Warren&Brandeis, Inc. Encargados de Tratamiento fuera de la UE, acogido a "Privacy Shield" +info...
Derechos	Acceder, rectificar y suprimir los datos, así como otros derechos, como se explica en la información adicional +info...
Información adicional	Puede consultar la información adicional y detallada sobre Protección de Datos en nuestra página web: http://www.warrenbrandeis.com/protecciondatos/info/

- Obsérvese que en el ejemplo se ha incluido, junto a la información básica facilitada, un hipervínculo que conduciría, en cada caso, al correspondiente epígrafe en la información adicional. Esta es una práctica recomendable siempre que se informe en medios electrónicos.

Ejemplo de Información básica en entrevista telefónica

- En una entrevista telefónica se deberá ofrecer la información básica como una **locución clara y concisa**, pero asegurando que el interlocutor **haya comprendido** la información suministrada, antes de proceder a la recogida de la información.
- Se ofertará poner a su disposición la información adicional por otro medio, pero si el interesado solicita alguna aclaración se le deberá ofertar una **locución complementaria** con la información adicional correspondiente al epígrafe sobre el que se haya interesado.

7 Información adicional (segunda capa)

- La información que se presente en la segunda capa ha de **completar con todos los detalles** la información resumida, así como **añadir la información adicional**, requerida por el RGPD y que no estaba presente en la primera capa.
- La información ofrecida en esta segunda capa debiera debe ser completa, es decir, no omitir información por el hecho de que ya se hubiese incluido en la información básica.

¿Por qué medios se puede facilitar la información adicional?

- La forma de presentar esta segunda capa también depende de las características del medio empleado para informar, si bien ya no debe estar condicionada en cuanto a la extensión de la información. Las posibilidades, en este caso, son más flexibles:

Información adicional en papel:

- ✓ En el mismo formulario cumplimentado (por ejemplo, en el reverso)
- ✓ Como un anexo o separata que se entregue al interesado y que pueda conservar
- ✓ Como información expuesta, claramente visible, en carteles, paneles, trípticos, etc, de los cuales se pueda solicitar una copia manejable para conservar.

Información adicional electrónica

- ✓ En una página web específica, a la que se accede mediante un hipervínculo
- ✓ Como un documento disponible para su descarga desde una URL
- ✓ Como información anexa o adjunta a un mensaje electrónico dirigido al interesado

Información adicional telefónica:

- ✓ Como una locución que se le ofrezca al interesado, como complemento o alternativa a una oferta de disponibilidad de información adicional accesible electrónicamente o remitida, por correo postal o electrónico.

¿Qué lenguaje utilizar?

- El lenguaje utilizado debe ser **claro, conciso, y comprensible**. A modo de sugerencia de estilo, se pueden seguir las siguientes directrices:
 - ✓ Se sugiere utilizar una exposición bien **estructurada**, en base a “preguntas y respuestas”, siguiendo los epígrafes generales antes descritos.
 - ✓ Se debe buscar un equilibrio entre **concisión y precisión**, evitando circunloquios, explicaciones innecesarias o detalles confusos
 - ✓ Se debe **evitar el abuso** de citas legales, “jerga” confusa, o términos ambiguos o con escaso sentido para las personas destinatarias

¿Qué información se debe incluir en cada epígrafe?

- La extensión y el nivel de detalle de cada epígrafe dependerán de la complejidad de sus circunstancias particulares. En los siguientes apartados se explican las variantes aplicables a cada uno de los epígrafes, incluyendo ejemplos prácticos relacionados con los casos hipotéticos anteriores (“*Ediciones Warren & Brandeis, S.A.*”).
- También puede **mejorarse** la transparencia y lealtad proporcionando voluntariamente información adicional, **no requerida por el RGPD**, respecto de:
 - ✓ Buenas prácticas, garantías y medidas adicionales aplicadas,
 - ✓ Usos y prácticas que expresamente se evitarán,con el fin de contribuir a mejorar la protección de los datos personales y a **generar confianza** en los interesados.

7.1 Epígrafe “Responsable”

- Aunque la identidad del responsable del tratamiento ya se habrá ofrecido en la información básica, en la información adicional se debe completar su información, incorporando los siguientes datos:
 - ✓ Identidad y datos de contacto del Responsable y, en su caso⁹, de su representante

⁹ Cuando el Responsable no esté establecido en la Unión Europea, deberá designar un representante en la Unión. Para más información, puede consultarse el artículo 27 RGPD

- ✓ Datos de contacto¹⁰ del Delegado de Protección de Datos, en su caso
- Como datos de contacto debe incluirse, en cada caso, una dirección **postal** y, si se dispone de ella, una dirección **electrónica**.
 - ✓ Resulta preferible proporcionar siempre una dirección postal **localizada**, sin perjuicio de que se facilite, además, un apartado postal.
 - ✓ La dirección electrónica puede ser, por ejemplo, una dirección de correo electrónico, o bien una URL que acceda a una aplicación o formulario electrónico para contactar.

▪ Ejemplo: **¿Quién es el Responsable del tratamiento de sus datos?**

Identidad: Ediciones Warren&Brandeis, S.A. - CIF: A01234566
Dir. postal: Calle Universidad de Harvard, nro. 5 - 28000 – Madrid
Teléfono: 912345678
Correo elect.: info@warrenbrandeis.com
Delegado de Protección de Datos:
Contacto DPD.: <https://www.warrenbrandeis.com/protecciondatos/dpd/>

7.2 Epígrafe “Finalidad”

- Además de la finalidad resumida ofrecida en la primera capa, debe informarse con mayor detalle de los **finés del tratamiento** a que se destinan los datos personales, incluyendo el **plazo** durante el cual se conservarán dichos datos personales o, cuando no sea posible, los **criterios** utilizados para determinar este plazo.
 - ✓ Debe tenerse en cuenta que el “*principio de limitación de la finalidad*” establece que los datos serán recogidos exclusivamente para fines **determinados, explícitos y legítimos**, y no serán tratados ulteriormente de manera incompatible con dichos fines.
 - ✓ Cuando se proyecte el tratamiento **ulterior** de datos personales para un fin **que no sea aquel** para el que se recogieron, se proporcionará al interesado, **con anterioridad** a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente.
- Asimismo, se informará de la existencia de **decisiones automatizadas**, incluida la elaboración de **perfiles** y, al menos en tales casos, se proporcionará información significativa sobre la lógica aplicada, así como la importancia y las **consecuencias** previstas de dicho tratamiento para el interesado¹¹.

¹⁰ No es preciso facilitar la identidad del Delegado de Protección de Datos, solamente sus datos de contacto

¹¹ Para más información sobre decisiones automatizadas, puede consultarse el artículo 22 RGPD

▪ Ejemplo : **¿Con qué finalidad tratamos sus datos personales?**

“En Warren & Brandeis tratamos la información que nos facilitan las personas interesadas con el fin de (...gestionar el envío de la información que nos soliciten.../...facilitar a los interesados ofertas de productos y servicios de su interés.../...)”

“Con el fin de (... poder ofrecerle productos y servicios de acuerdo con sus intereses.../... mejorar su experiencia de usuario...), elaboraremos un “perfil comercial”, en base a la información facilitada. No se tomarán decisiones automatizadas en base a dicho perfil.”

¿Por cuánto tiempo conservaremos sus datos?

“Los datos personales proporcionados se conservarán (...mientras se mantenga la relación mercantil, .../... no se solicite su supresión por el interesado.../...durante un plazo de xx años a partir de la última confirmación de interés...)”.

- Deben evitarse prácticas tales como incluir finalidades demasiado genéricas o inespecíficas, que puedan conducir a tratamientos posteriores que excedan las expectativas razonables del interesado.

7.3 Epígrafe “Legitimación”

- Como ya se ha indicado respecto de la información básica, este epígrafe se refiere a la base jurídica en la cual se basa el tratamiento. Además de la información básica ofrecida en la primera capa, será necesario indicar aquí, según el caso:

Legitimación por ejecución de un contrato:

- ✓ Cuando el tratamiento sea necesario para la ejecución de algún contrato (mercantil, laboral, administrativo,...) en el que el interesado sea parte, o para la aplicación de medidas precontractuales, **se hará constar una referencia al contrato** o tipo de contrato de que se trate, con el detalle suficiente para que no quepa ninguna ambigüedad sobre lo que se refiere.

Legitimación por cumplimiento de una obligación legal:

- ✓ Cuando el tratamiento sea necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento, es decir, una obligación derivada del derecho de la Unión o del ordenamiento jurídico interno, **deberá hacerse constar, sin ambigüedad, cuál es la norma**, con rango de Ley, que impone la obligación.

Legitimación por misión en Interés público o ejercicio de Poderes Públicos:

- ✓ Cuando el tratamiento sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (como ocurre en el caso del Sector Público), igualmente **se hará constar, sin ambigüedad, cuál es la norma**, con rango de Ley, que confiere los poderes públicos o califica la misión como de interés público.

Legitimación por Interés legítimo del Responsable, o de un tercero:

- ✓ Cuando el tratamiento sea necesario para la satisfacción de “intereses legítimos” perseguidos por el responsable del tratamiento o por un tercero, **se explicitarán cuáles son tales intereses**. Se considera una buena práctica incluir un resumen de la ponderación de su legitimidad¹² frente a los intereses y los derechos y libertades fundamentales del interesado, cuando ello contribuya al principio de transparencia.

Legitimación por consentimiento del interesado:

- ✓ Cuando la legitimación para la finalidad principal no encuentre acomodo en **ninguna de las bases jurídicas anteriores**, deberá solicitarse el consentimiento del interesado para el tratamiento de sus datos personales, y **así se hará constar** en este apartado¹³.
 - ✓ En el caso de que la finalidad principal sí esté legitimada por alguna de las bases jurídicas antes apuntadas, pero alguna **finalidad específica** requiera del consentimiento del afectado, **se harán constar ambas** legitimaciones.
 - ✓ En este último caso, se debería informar al interesado de que la finalidad principal, **no está supeditada al consentimiento** de los datos que no sean necesarios para dicha finalidad principal, puesto que de lo contrario el consentimiento no tendría la consideración de “*otorgado libremente*”.
- Si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, como puede ocurrir en los tres primeros supuestos de legitimación, deberá informarse **si el interesado está obligado** a facilitar los datos personales, así como de **las consecuencias de no hacerlo**.
 - Finalmente, entre las posibilidades de legitimación para el tratamiento, el RGPD también incluye la “**protección de intereses vitales**” del interesado o de otra persona. No se ha incluido entre las causas de legitimación por entender que se trata de un supuesto **residual**, aplicable a situaciones **especiales, urgentes o sobrevenidas**, y no debe constituir la causa de legitimación general de un tratamiento.

▪ Ejemplo: **¿Cuál es la legitimación para el tratamiento de sus datos?**

“La base legal para el tratamiento de sus datos es la ejecución del contrato de suscripción a las revistas que figuran en su cartera de pedidos (... según los términos y condiciones que constan en ...)”

La oferta prospectiva de productos y servicios está basada en el consentimiento que se le solicita, sin que en ningún caso la retirada de esta consentimiento condicione la ejecución del contrato de suscripción”

¹² La determinación sobre cuándo un determinado interés del Responsable puede calificarse de “legítimo” excede el objeto de esta guía. Para ampliar información puede consultarse el Dictamen 06/2014 del “Grupo del Artículo 29” sobre el concepto de interés legítimo, en la URL:

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_es.pdf

¹³ Las condiciones de la gestión del consentimiento excede el objeto de esta guía. Para ampliar información puede consultarse el Dictamen 15/2011 del “Grupo del Artículo 29” sobre la definición del consentimiento, en la URL:

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_es.pdf

- Deben evitarse prácticas tales como incorporar casillas pre-marcadas en los procedimientos de gestión del consentimiento, teniendo en cuenta el requisito impuesto por el RGPD de que el consentimiento deba otorgarse mediante una **clara acción afirmativa** que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado.

7.4 Epígrafe “Destinatarios”

- Cuando se haya previsto ceder o comunicar, legítimamente, los datos personales que se recogen, se informará acerca de la identidad de los destinatarios, si están claramente predeterminados, o de las categorías de destinatarios, si estos no están determinados previamente.
- En particular, es conveniente informar también de la existencia de Encargados de Tratamiento, cuya legitimidad del tratamiento es la ejecución del contrato del encargo, especialmente en los casos en que impliquen transferencias a terceros países.

▪ Ejemplo: **¿A qué destinatarios se comunicarán sus datos?**

“Los datos se comunicarán a otras empresas del grupo empresarial Warren&Brandeis, Inc. para fines administrativos internos, incluido el tratamiento de datos personales de clientes o empleados”.

“Warren&Brandeis, Inc dispone de Normas Corporativas Vinculantes, aprobadas por el Comité Europeo de Protección de Datos y disponibles en: <https://www.warrenbrandeis.com/protecciondatos/bcr/>

“Warren&Brandeis S.A contrata su infraestructura virtual según un modelo de “computación en la nube” a través de AWS y al amparo del acuerdo EU-US Privacy Shield. - Información disponible en:

<https://www.privacyshield.gov/participant?id=a2zt0000000TOWQAA4>

- Cuando se haya previsto transferir datos personales a un tercer país u organización internacional, se deberá informar a los interesados, además, de las condiciones que afectan a la transferencia, en particular, la existencia o ausencia de una decisión de adecuación de la Comisión respecto del tercer país u organización internacional.
- Cuando el responsable aporte garantías adecuadas o apropiadas, se informará de las mismas y de los medios para obtener una copia de estas o al hecho de que se hayan prestado. Tales garantías podrán ser, en particular:
 - ✓ instrumentos jurídicamente vinculantes entre las autoridades u organismos públicos
 - ✓ normas corporativas vinculantes¹⁴, dentro de un grupo empresarial
 - ✓ cláusulas tipo de protección de datos
 - ✓ códigos de conducta
 - ✓ mecanismos de certificación

¹⁴ «normas corporativas vinculantes»: “las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta”

7.5 Epígrafe “Derechos”

- En este epígrafe se deberá ofrecer la información sobre los derechos que le asisten a las personas interesadas, en relación con el Responsable, de acuerdo con el RGPD y que son:
 - ✓ Derecho a solicitar el acceso a los datos personales relativos al interesado,
 - ✓ Derecho a solicitar su rectificación o supresión,
 - ✓ Derecho a solicitar la limitación de su tratamiento, y a
 - ✓ Derecho a oponerse al tratamiento,
 - ✓ Derecho a la portabilidad de los datos;
- El Responsable deberá informar claramente sobre cómo puede el interesado **ejercer materialmente** estos derechos, mediante la puesta a su disposición de modelos o formularios y explicitando la forma de ponerse en contacto para formular su solicitud. Opcionalmente, puede redirigir al interesado a la Autoridad de Control competente para obtener información adicional acerca de sus derechos.
- También deberá informar, en el caso de que se haya otorgado el consentimiento para alguna finalidad específica, que tiene derecho a **retirar el consentimiento** en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada.
- Asimismo, deberá informar a los interesados de que pueden **presentar una reclamación** ante la Autoridad de Control en materia de Protección de Datos competente, especialmente cuando no haya obtenido satisfacción en el ejercicio de sus derechos, y la forma de ponerse en contacto con ella.

- Ejemplo: **¿Cuáles son sus derechos cuando nos facilita sus datos?**
 - *“Cualquier persona tiene derecho a obtener confirmación sobre si en Warren&Brandeis estamos tratando datos personales que les conciernan, o no.*
 - *Las personas interesadas tienen derecho a si acceder a sus datos personales, así como a solicitar la rectificación de los datos inexactos o, en su caso, solicitar su supresión cuando, entre otros motivos, los datos ya no sean necesarios para los fines que fueron recogidos.*
 - *En determinadas circunstancias, los interesados podrán solicitar la limitación del tratamiento de sus datos, en cuyo caso únicamente los conservaremos para el ejercicio o la defensa de reclamaciones.*
 - *En determinadas circunstancias y por motivos relacionados con su situación particular, los interesados podrán oponerse al tratamiento de sus datos. Warren&Brandeis dejará de tratar los datos, salvo por motivos legítimos imperiosos, o el ejercicio o la defensa de posibles reclamaciones.*
 - (...)

- En el ejemplo anterior no han sido contemplados todos los supuestos. No pretende agotar las posibilidades de información ni constituir un modelo aplicable a cualquier tratamiento sino, por el contrario, pretende únicamente ilustrar un posible estilo de información en unos casos concretos, con la información mínima que debiera ofrecerse.

7.6 Epígrafe “Procedencia”

- El epígrafe sobre la procedencia de los datos únicamente habrá de incluirse en el supuesto de que los datos personales no se hayan obtenidos del interesado, por proceder de alguna cesión legítima, o de fuentes de acceso público.
- Los medios para facilitar esta información serán, normalmente, diferentes a los utilizados para informar en el momento de recoger los datos. Los más adecuados pueden ser:
 - ✓ Correo postal
 - ✓ Correo electrónico
 - ✓ Mensajería instantánea

Habrà de ponderarse la adecuaci3n del medio con la necesidad de poder demostrar que se ha dado cumplimiento al deber de informa.

- En el caso del correo postal o del correo electr3nico, la pràctica que se sugiere como màs adecuada es:
 - ✓ incorporar la informaci3n bàsica en la propia notificaci3n donde se le informa al interesado del tratamiento, ampliada con el epígrafe resumido de “Procedencia”
 - ✓ adjuntar la informaci3n adicional o completa como un anexo o separata, incluyendo el epígrafe ampliado de “Procedencia”
 - ✓ opcionalmente, incluir una vinculaci3n a la informaci3n adicional en forma electr3nica
- En el caso de la mensajería instantánea, este medio únicamente permite incluir una breve referencia a la naturaleza de la comunicaci3n, màs una vinculaci3n a la informaci3n adicional en forma electr3nica, por lo que únicamente debiera utilizarse cuando no exista otra posibilidad. Tampoco parece adecuado informar telef3nicamente mediante una locuci3n.
- La informaci3n a facilitar es, en este caso:
 - ✓ la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso pùblico disponibles sin restricciones
 - ✓ las categorías de datos personales de que se trate, con especial indicaci3n de los datos especialmente protegidos.

- Ejemplo: **¿C3mo hemos obtenido sus datos ?**
- *Los datos personales que tratamos en Warren&Brandeis S.A proceden de otras empresas del grupo Warren&Brandeis Inc.*
- Las categorías de datos que se tratan son:
 - Datos de identificaci3n
 - C3digos o claves de identificaci3n
 - Direcciones postales o electr3nicas
 - Informaci3n comercial
 - Datos econ3micos
- No se tratan datos especialmente protegidos

AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS



apdcat

Autoritat Catalana de Protecció de Dades



Datuak Babesteko
Euskal Bulegoa
Agencia Vasca de
Protección de Datos

EN REVISIÓN