www.pwc.es

Nuevo Reglamento de Protección de Datos (RGPD)

MAS MOTOR CANARIAS, S.L.

CANARIOALEMANA DE AUTOMÓVILES S.L.

PELICAN MOTOR, S.L

pwc

Índice

01

Introducción

1.1. Evolución de la normativa en materia de protección de datos

En España contamos con la **Ley Orgánica 15/1999,** de 13 de diciembre, de Protección de Datos de Carácter Personal ("**LOPD**") y el **Real Decreto 1720/2007**, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley ("**RLOPD**").

El nuevo **Reglamento General de Protección de Datos de la UE** ("**RGPD**") es una norma directamente aplicable en todos los estados miembros. Por tanto, desde **el 25 mayo de 2018**, todas las disposiciones de este Reglamento deben cumplirse en España.

Una de las principales novedades que trae consigo RGPD es el régimen sancionador.

Las **multas económicas** en el RGPD se **incrementan sustancialmente** respecto a los rangos establecidos en la LOPD, pudiendo alcanzar hasta **20.000.000 EUR** o hasta 4% del volumen total del negocio mundial de la compañía.

1.2. Nuevo régimen sancionador

Las multas económicas en el RGPD **se incrementan sustancialmente** respecto a los rangos establecidos en la LOPD, pudiendo alcanzar:

Hasta **10.000.000 EUR** o hasta **2% del volumen total** del negocio mundial de la compañía infractora en el ejercicio anterior por infracciones relativas a	Hasta **20.000.000 EUR** o hasta **4% del volumen total** del negocio mundial de la compañía infractora en ejercicio anterior por infracciones relativas a
• Incumplimiento de las obligaciones del responsable y encargado; • Obligaciones de los organismos de certificación; • Obligaciones de la autoridad de control;	• Principios básicos del tratamiento; • Derechos de los interesados; • Transferencias de datos personales; • Toda obligación en virtud del Derecho de los EEMM relativa a sitaciones específicas de tratamiento; • Incumplimiento de una resolución o de una limitación temporal o definitiva del tratamiento o la suspension de los flujos de datos por la autoridad de control; • Incumplimiento de las resoluciones de la autoridad de control;

**Los EEMM podrán determinar normas sobre si se puede y en qué medida, imponer multas administrativas a autoridades y organismos públicos.*

Es aconsejable que el responsable del tratamiento determine de inicio una **estrategia de actuación frente a potenciales situaciones de incumplimiento** en función de su propia situación e intereses. Esta estrategia puede llegar incluso a tomar la decisión de provisionar determinadas cantidades para afrontar la defensa y, en su caso, pago de potenciales sanciones.

1.3. ¿Qué es y qué no es un dato personal? (i)

Dato personal

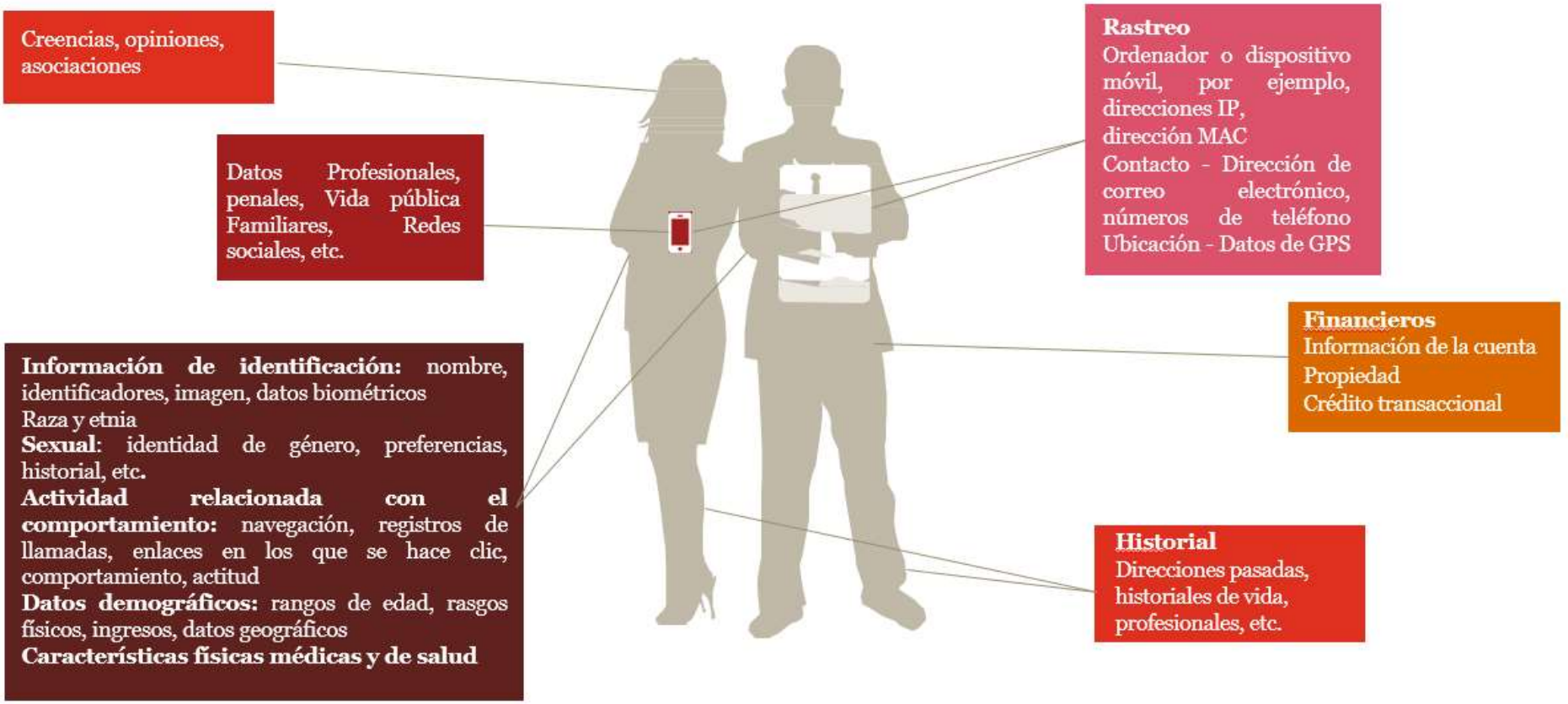
Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables

A tales efectos, se entiende por **persona física identificable** toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social.

- Imagen
- DNI
- Voz
- E-mail

En definitiva, cualquier información que pueda permitir identificar a una persona física de manera sencilla será considerada un dato de carácter personal. El nombre y apellidos de una persona, sus iniciales, su número de DNI, su dirección postal, su correo electrónico, su dirección IP, su información bancaria o una fotografía en la que aparezca su rostro pueden ser datos de carácter personal, entre otros ejemplos.

1.3. ¿Qué es y qué no es un dato personal? (ii)



1.3. ¿Qué es y qué no es un dato personal? (iii)

Entonces, ¿Qué tipo de información no sería un dato personal?

Como se ha visto, **la legislación no determina un listado cerrado de datos de carácter personal**, sino que establece una definición abierta, en la que tienen cabida diferentes conceptos. No obstante lo anterior, existen algunos tipos de información que, por regla general, podemos determinar que no serían datos de carácter personal:

Datos concernientes a personas jurídicas (como sociedades mercantiles)

Datos anonimizados o disociados

Información que no se refiera a ninguna persona física

Know how y procedimientos empresariales (que no contengan información de personas físicas)

1.4. La figura del responsable y del encargado del tratamiento (i)

Definiciones

Responsable del tratamiento: persona física o jurídica, autoridad pública u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento de datos personales.

* **Ejemplo:** CANAAUTO sería responsable del tratamiento de los datos de sus clientes.

Encargado del tratamiento: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

* **Ejemplo:** un proveedor que accede a datos de la empresa en el ámbito de una prestación de servicios.

Si el encargado a su vez subcontrata parte de los servicios, nos encontraríamos con un **sub-encargado del tratamiento**.

1.4. La figura del responsable y del encargado del tratamiento (ii)

Responsables del Tratamiento

Según el RGPD, el responsable deberá adoptar medidas apropiadas, incluida la elección de encargados, de forma que garantice y esté en condiciones de demostrar que el tratamiento se realiza conforme el RGPD (**principio de responsabilidad activa**).

Por ello, el Concesionario deberá elegir encargados que ofrezcan **garantías suficientes** para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del Reglamento. En este sentido, las relaciones entre el responsable y el encargado deben formalizarse siempre en un contrato que vincule al encargado respecto al responsable, debiendo preverse aspectos tales como:

- **Objeto**, duración, naturaleza y la **finalidad** del tratamientos;

- **Tipología** de datos personales y categorías de **interesados**;

- **Condiciones** para que el responsable pueda dar su autorización previa, específica o general, a las subcontrataciones, atención de **derechos** de interesados, **brechas** de seguridad, etc.

1.4. La figura del responsable y del encargado del tratamiento (iii)

Encargados de Tratamiento

En determinadas materias, el concesionario, puede actuar como encargado del tratamiento debiendo asumir obligaciones propias que establece el RGPD, que no se circunscriben al ámbito del contrato que los une al responsable, y que pueden ser supervisadas separadamente por las autoridades de protección de datos. Por ejemplo:

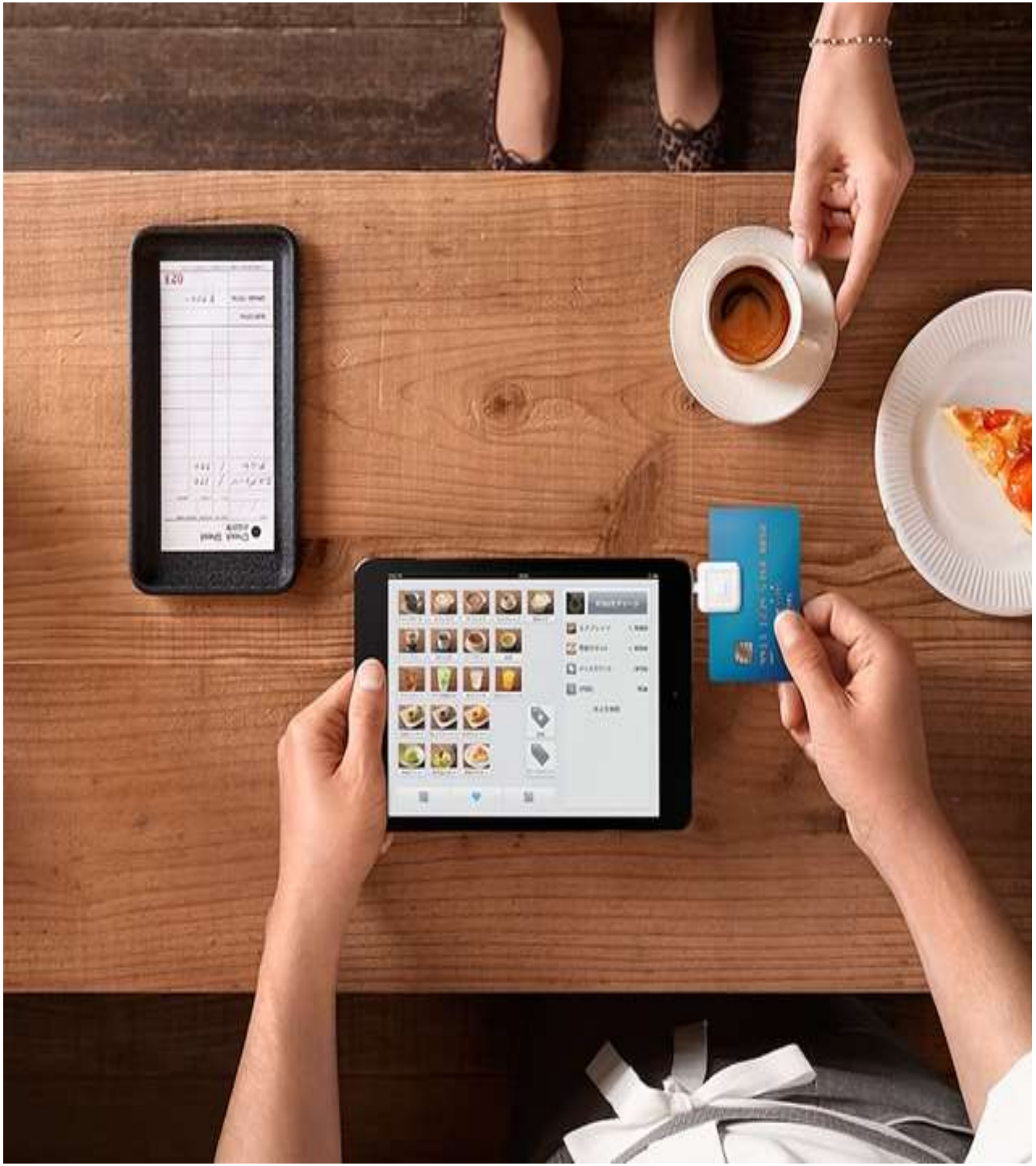
• Deben mantener un **registro de actividades** de tratamiento.

• Deben determinar las **medidas de seguridad** aplicables a los tratamientos que realizan.

• Deben designar a un **Delegado de Protección de Datos** en los casos previstos por el RGPD.

02

Principales novedades para el Concesionario

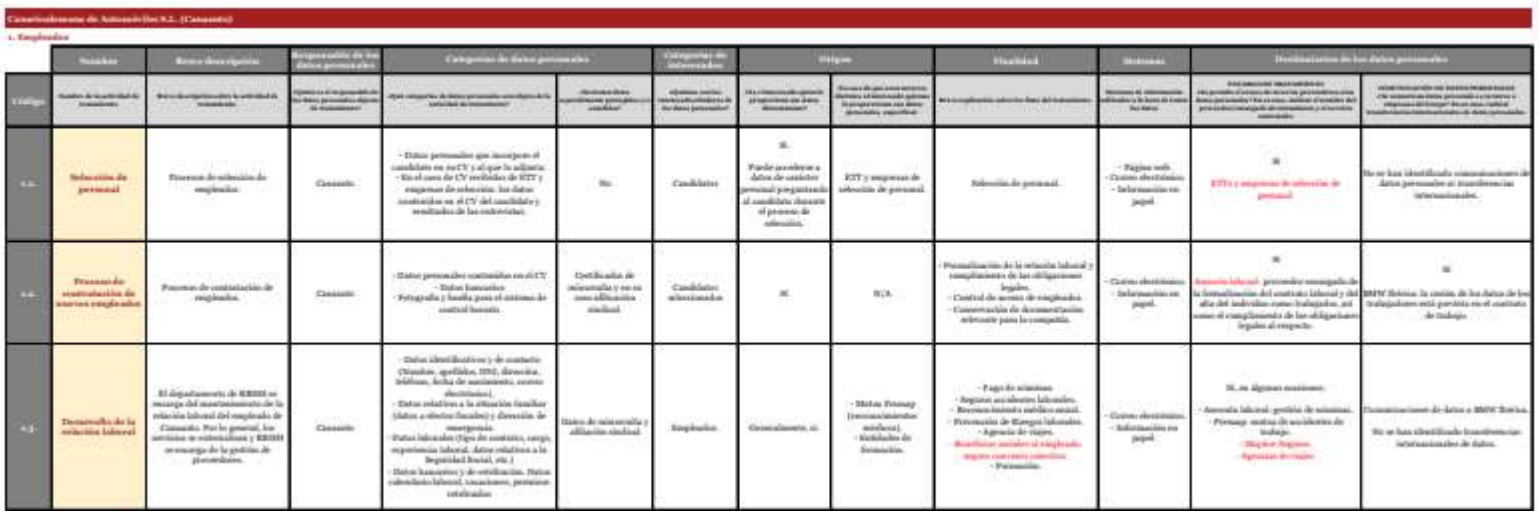


2.1. Principales novedades del RGPD

2.2. Registro de actividades del tratamiento

El **artículo 30 del Reglamento General de Protección de Datos** establece que cada responsable del tratamiento debe llevar a cabo un **registro de todas las actividades de tratamiento** que realice en el seno de su actividad.

En este sentido, el Concesionario cuenta actualmente con el siguiente registro de actividades de tratamiento como responsable:

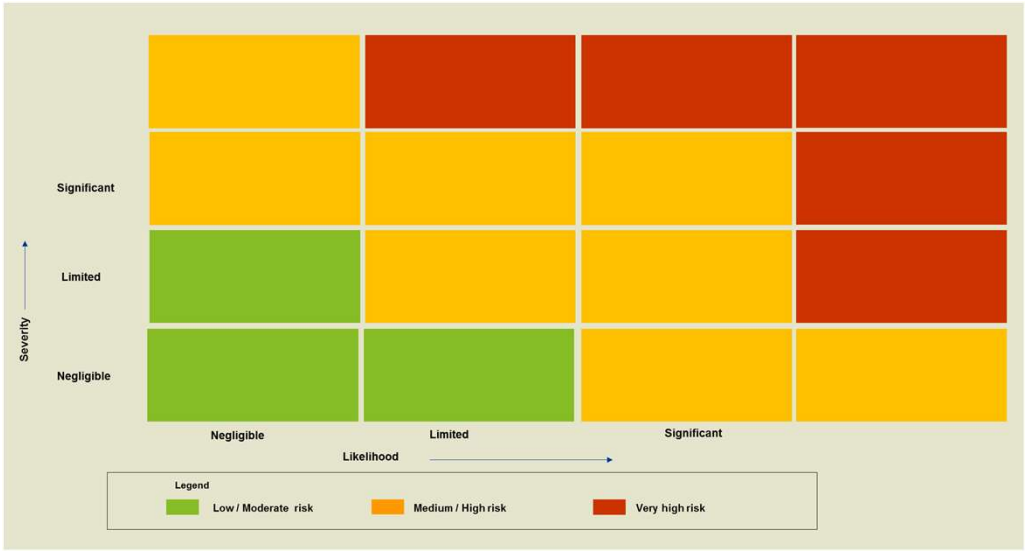


Ejemplo de registro de actividades que el Concesionario mantiene como responsable del tratamiento

2.3. Valoración objetiva del riesgo

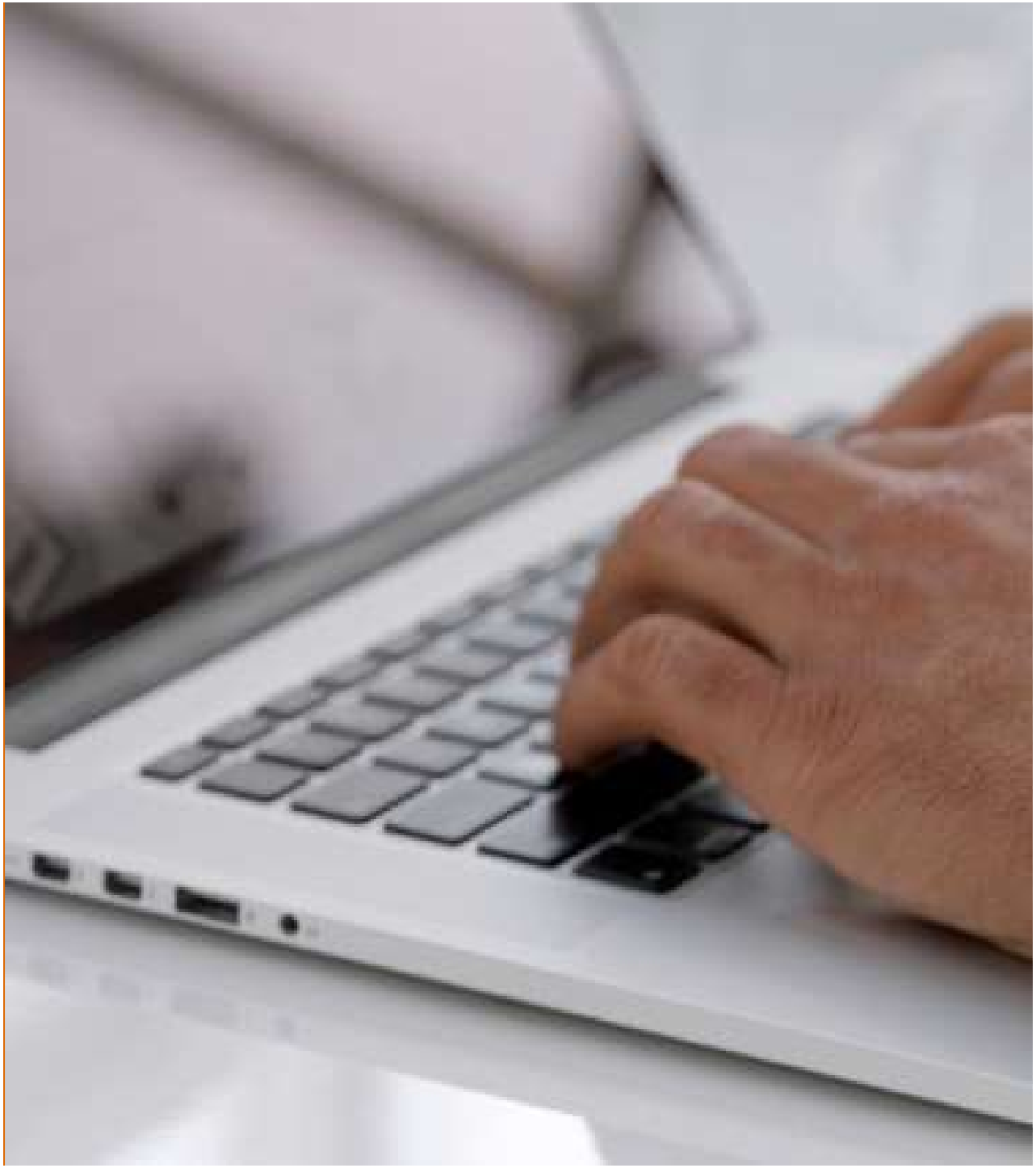
El **Reglamento General de Protección de Datos** establece la necesidad de que se realice una **valoración objetiva de los riesgos para la privacidad de las personas** de cada uno de los tratamientos. Esto es de especial relevancia, ya que en caso de existir algún tratamiento de riesgo alto, debería realizarse una "Evaluación de impacto relativa a la protección de datos" (PIA).

No obstante lo anterior, dada la naturaleza de las actividades realizadas por el Concesionario no se ha considerado necesario elaborar un PIA.



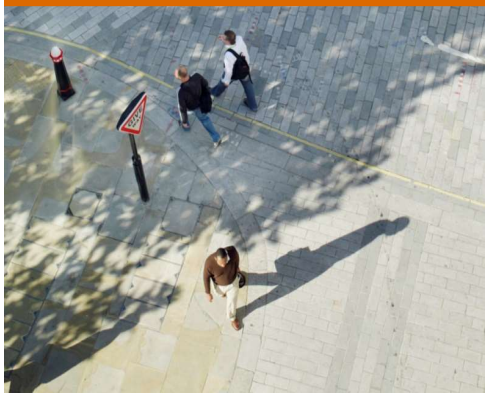
03

Otras cuestiones relevantes del RGPD



3.1. Principio de Accountability y Privacy-by-design (i)

Principio de Accountability



El responsable del tratamiento debe aplicar medidas técnicas y organizativas apropiadas para **poder garantizar y demostrar** que el tratamiento que realiza es conforme con el RGPD, teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos para los derechos y libertades de las personas físicas. Entre las nuevas obligaciones cuyas obligaciones deben ser probadas se incluyen entre otras:

3.1. Principio de Accountability y Privacy-by-design (ii)

La nueva realidad del privacy-by-design

Se exigirá a los responsables del tratamiento de datos, de nuevas obligaciones relacionadas con la adopción de **medidas técnicas y organizativas apropiadas** (como la seudoanonimización), tanto en el **momento** en el que se determinen los medios de tratamiento, como en el momento propio del tratamiento de los datos.

Las entidades que traten datos personales deberán elaborar una estrategia, previa al tratamiento de los datos, para diseñar las medidas que sea necesario adoptar en función del tratamiento correspondiente (**Privacy-by-design**) y que deberán aplicarse en la fase de desarrollo, diseño y uso de aplicaciones, servicios o productos.

Estas medidas deberán garantizar que, por defecto (**Privacy-by-default**), sólo sean objeto de tratamiento los datos personales exclusivamente necesarios para cada uno de los fines específicos del tratamiento.

El responsable del tratamiento no va a poder obviar los riesgos derivados de los tratamientos de datos. Deberá identificar dichos riesgos en relación a cada nuevo lanzamiento de productos o servicios que implique un acceso a datos personales a fin de determinar su alcance, involucrando a todas las áreas de la compañía afectada.

3.2. Deber de información y consentimiento (i)

¿Qué es el "deber de información"?

Para poder obtener adecuadamente el consentimiento (que se estudiará más adelante) y, como consecuencia, llevar a cabo el tratamiento de los datos personales de una persona, **la legislación establece que es necesario informar previamente** de todos los pormenores de dicho tratamiento.

Un ejemplo de cumplimiento de este deber de información serían las cláusulas informativas a incluir en la **hoja de un pedido**, la **orden de reparación** o la **Política de Privacidad** que encontramos en páginas web como la de Mas Motor Canarias, S.L.

Política de privacidad

Datos de los Responsables

Los datos personales serán tratados por MÁS MOTOR CANARIAS SL, con domicilio en Calle las Industrias 14, 38108, La Laguna, Santa Cruz de Tenerife (en adelante, el "Miembro de la Red Ford") y Ford España, S.L., con domicilio social en la calle Caléndula 13, 28109, Alcobendas, Madrid y CIF. B-46066361.

Objeto de la Política de Privacidad

La presente Política de Privacidad tiene por objeto informar de la forma y los fines para los que el Miembro de la Red Ford y Ford España, S.L. (en adelante, "Ford" y ambos, el Miembro de la Red Ford y Ford, "nosotros", o "nos"), recaba, trata y explica la utilización de sus datos personales obtenidos cuando se ha visitado o facilitado a través de este sitio web (en adelante, el "Sitio Web") o se hayan recabado en el contexto de la adquisición de un producto o servicio de Ford.

3.2. Deber de información y consentimiento (ii)

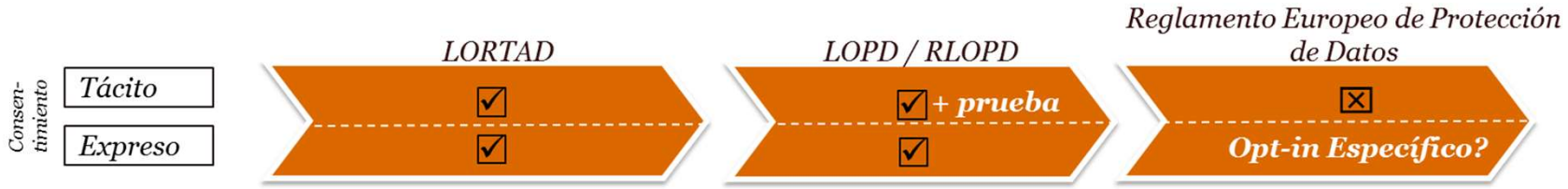
¿De qué es necesario informar según el RGPD?

El nuevo RGPD amplía la información que el responsable del tratamiento debe ofrecer al interesado de manera previa a recabar sus datos:

a)	Identidad y datos de contacto del responsable;	g)	Plazo de conservación de los datos;
b)	Datos de contacto del delegado de protección de datos;	h)	Derecho de acceso, rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;
c)	Fines del tratamiento y base jurídica del tratamiento;	i)	Derecho a retirar el consentimiento (si aplica);
d)	Intereses legítimos del responsable (en caso de que el tratamiento se base en esta circunstancia);	j)	Derecho a presentar una reclamación ante una autoridad de control;
e)	Destinatarios o categorías de destinatarios de los datos personales;	k)	Si: • la comunicación de datos es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y • el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias;
f)	Intención del responsable de transferir los datos personales a un tercer país y la existencia o ausencia de una decisión de adecuación de la Comisión, o referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de éstas o al hecho de que se hayan prestado;	l)	La existencia de decisiones automatizadas;

3.2. Deber de información y consentimiento (iii)

¿Cómo ha de obtenerse el consentimiento de los interesados?



Cuando el consentimiento se obtenga por medio de un documento en el que se incluyan referencias a otros asuntos (por ejemplo, términos y condiciones de contratación), debe presentarse de forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso.

Según el RGPD, serían modos válidos para obtener el consentimiento:

- Marcar una casilla de un sitio web en internet.
- Escoger parámetros técnicos para la utilización de servicios de la sociedad de la información.
- Cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales.

Por tanto, según el RGPD, **el silencio, las casillas marcadas por defecto o la inacción no serían medios válidos** para otorgar el consentimiento. Asimismo, el RGPD establece que el consentimiento debe darse para todas las actividades de tratamiento realizadas con los mismos fines. De esta manera, cuando el tratamiento cuente con distintas finalidades, **debe darse el consentimiento para todas ellas**.

3.3. Base legitimadora

Según el RGPD, para poder tratar los datos de cualquier persona, es necesario **contar con una base que nos legitime para ello**. La base legitimadora más garantista y común es **el consentimiento**, aunque existen otras posibles bases legitimadoras que permitirían igualmente tratar los datos:

- **Consentimiento.** La persona ha otorgado su consentimiento expreso. Una de las novedades más importantes introducidas por el RGPD es que el interesado debe otorgar el consentimiento mediante una **clara acción afirmativa**, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal.

- **Ejecución de un contrato.** El tratamiento es necesario para **ejecutar un contrato**. Ejemplo: tratamiento de datos de empleados para la contratación.

- **Cumplimiento de una obligación legal.** El tratamiento es necesario para cumplir con una **obligación legal** del responsable. Ej: ceder datos a la Seguridad Social.

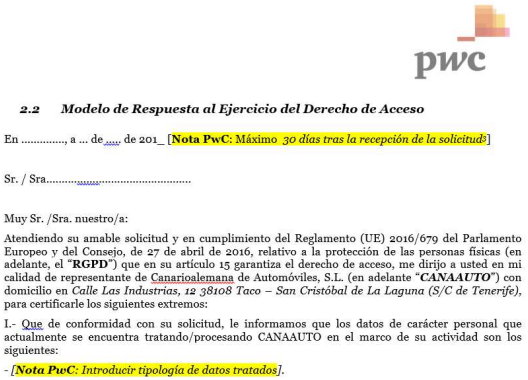
- **Interés legítimo.** El tratamiento es necesario para la satisfacción de un **interés legítimo** del responsable. En este caso será necesario evaluar que este prevalezca sobre los derechos de los interesados. Ejemplo: prevención del fraude o tratamiento de datos de clientes y proveedores en relaciones B2B (art. 19 Proyecto de nueva LOPD).

3.4. Derechos de los interesados

Los interesados cuyos datos se traten pueden ejercitar los siguientes derechos de protección de datos:

- **Acceso**
- **Rectificación**
- **Portabilidad**
- **Supresión y olvido**
- **Oposición**
- **Decisiones automatizadas**

Estos derechos pueden ser ejercitados por empleados o clientes. A estos efectos, el Concesionario cuenta con un protocolo de respuesta que **explica los pasos a seguir e incluye un modelo de respuesta** para cada uno de los derechos.



2.2 Modelo de Respuesta al Ejercicio del Derecho de Acceso

En ....., a ... de ...., de 201_ [**Nota PwC**: Máximo *30 días tras la recepción de la solicitud*[3]]

Sr. / Sra.....

Muy Sr. /Sra. nuestro/a:

Atendiendo su amable solicitud y 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 adelante, el "**RGPD**") que en su artículo 15 garantiza el derecho de acceso, me dirijo a usted en mi calidad de representante de Canarioalemana de Automóviles, S.L. (en adelante "***CANAAUTO***") con domicilio en *Calle Las Industrias, 12 38108 Taco – San Cristóbal de La Laguna (S/C de Tenerife)*, para certificarle los siguientes extremos:

I.- Que de conformidad con su solicitud, le informamos que los datos de carácter personal que actualmente se encuentra tratando/procesando CANAAUTO en el marco de su actividad son los siguientes:

- [***Nota PwC**: Introducir tipología de datos tratados*].

3.5. Delegado de Protección de Datos (i)

Ámbito objetivo

01 ***Actividad principal***: aquella relacionadas con actividades primarias y no con el tratamiento de datos personales con actividades auxiliares

Tratamientos a gran escala: monitorización de hábitos de navegación, utilización de sistema de geolocalización, tratamiento de datos de clientes por entidades financieras o del tráfico de redes de comunicaciones por el Concesionario 02

03 El DPO puede desempeñar otras tareas y funciones pero se tiene que evitar el conflicto de intereses (no puede ocupar puestos de alta dirección)

Sistema de certificación de profesionales de protección por parte de la AEPD. 04

05 Se permite que el DPO mantenga una relación laboral o mercantil (prestación de servicios, a tiempo completo o parcial). Puede haber un DPO para una empresa o Grupo empresarial

Debe tener conocimiento de las leyes y practicas de protección de datos nacionales y europeas. Suficiente comprensión de los sistemas de información y seguridad 06

3.5. Delegado de Protección de Datos (ii)

No obstante, teniendo en cuenta que en el Concesionario:

- ✓ **No** se tratan datos de carácter personal que requieran una **observación habitual y sistemática de interesados** a gran escala, y
- ✓ **No se tratan datos especialmente protegidos** o, en su caso, el tratamiento no se lleva a cabo a gran escala.

CANAAUTO, MAS MOTOR y PELICAN MOTOR no estarían obligados a designar un DPD ni, consecuentemente a cumplir con las respectivas obligaciones formales establecidas por el RGPD y el Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal, así como con las consideraciones que en su caso establezca la Agencia Española de Protección de Datos.

04

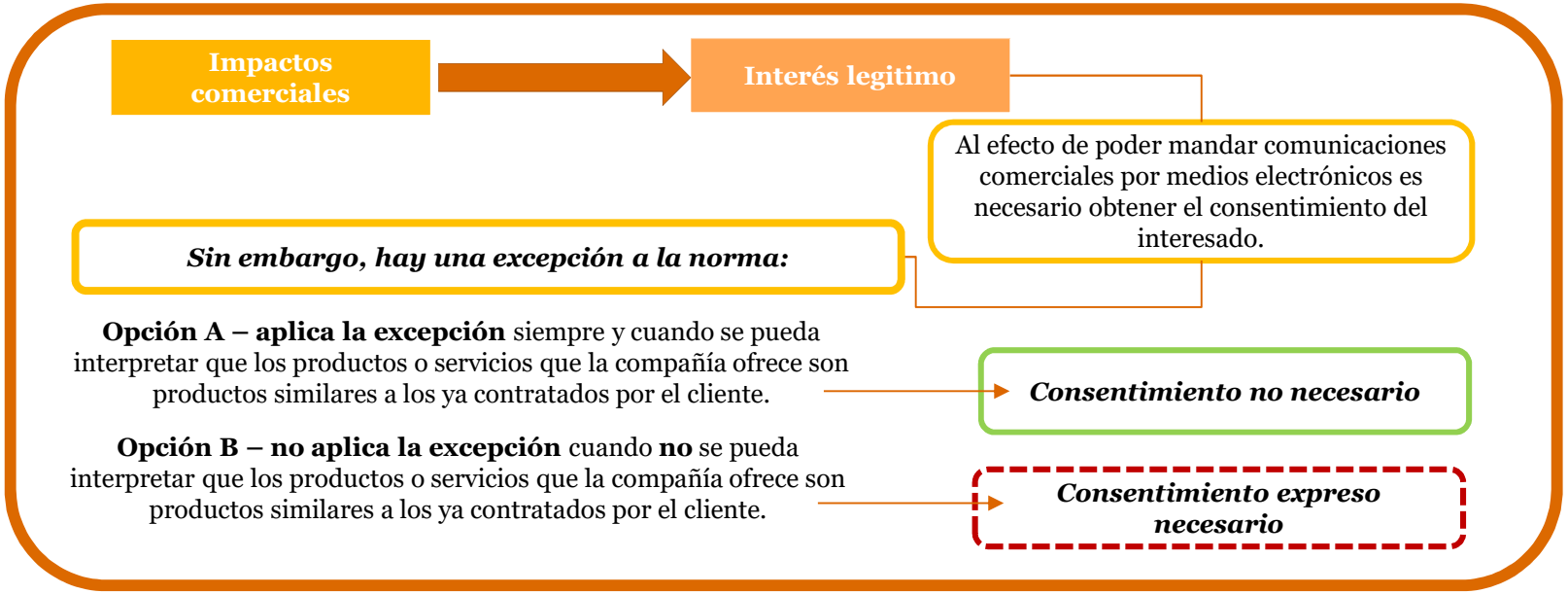
Impacto para el Concesionario en el día a día

4.1. Comunicaciones comerciales (i)

Comunicaciones comerciales.

Las comunicaciones comerciales que se remitan tienen que estar amparadas por una base legitimadora, bien sea por el consentimiento expreso otorgado por la persona a quien vayan dirigidas dichas comunicaciones o por el interés legitimo del Concesionario.

Se podrían entender amparadas por el interés legitimo del Concesionario aquellas comunicaciones a clientes de la compañía sobre productos similares a los que estos ya hayan contratado.



4.1. Comunicaciones comerciales (ii)

Leads

	Mas Motor Ford Go Further	BMW Canaauto	Jaguar Pelican Motor Land Rover
Solicitud de oferta	**Mas Motor y Ford son <u>corresponsables</u> del tratamiento**, por tanto, <u>no habrá cesión de datos a la marca.</u> • Comunicaciones comerciales de ambos: **Consentimiento**	• Comunicaciones comerciales sobre **productos de Canaauto**: **Consentimiento** • **Cesión de datos** a Grupo BMW: **Consentimiento**	• Comunicaciones comerciales sobre **productos de Pelican**: **Consentimiento** • **Cesión de datos** a Grupo JLR: **Consentimiento**
Hoja de pedido	• Comunicaciones comerciales de ambos: **Consentimiento**	• Comunicaciones comerciales sobre **productos de Canaauto**: **Informar** • Comunicaciones comerciales haciendo un **perfilado**: **Consentimiento** • Comunicaciones comerciales sobre **productos del Grupo BMW** u otras entidades: **Consentimiento** • **Cesión de datos** a Grupo BMW: **Consentimiento**	• Comunicaciones comerciales sobre **productos de Pelican**: **Informar** • **Cesión de datos** a Grupo JLR: **Consentimiento**
Clientes post - venta			

4.1. Comunicaciones comerciales (iii)

Bases de datos.

Con RGPD una compañía únicamente puede realizar comunicaciones comerciales a los clientes amparados por las bases legitimadoras antes mencionadas.

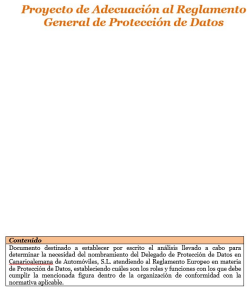
En este sentido cabe destacar que dichas bases legitimadoras permiten la comunicación comercial exclusivamente a la compañía que cuenta con el consentimiento expreso o bien con el interés legitimo para realizarla.

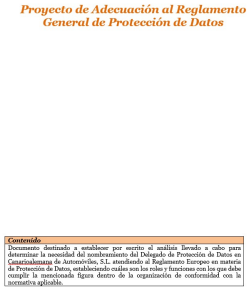
En ningún caso se podrán utilizar bases de datos de otras sociedades en una sociedad para la cual no se han obtenido los consentimientos de los interesados ni se cuenta con una base legitimadora.

4.2. Metodología de adecuación al RGPD (i)

Al efecto de implantar de manera adecuada el RGPD se han creado unos protocolos de actuación para el Concesionario.

En este sentido, cabe destacar el procedimiento a realizar en el supuesto en que aparezca una brecha de seguridad y el procedimiento a seguir a la hora de contratar nuevos proveedores.





Asimismo hay que tener en consideración que, tanto en los documentos suscritos históricamente por el Concesionario como en los nuevos documentos que se hayan de suscribir, hay que modificar las menciones a la LOPD por RGPD así como adaptar el contenido de los mismos al nuevo reglamento.

RGPD permite adaptar los documentos históricos en el momento de renovarlos, sin ser necesario adaptarlos de manera inmediata.

4.2. Metodología de adecuación al RGPD (ii)

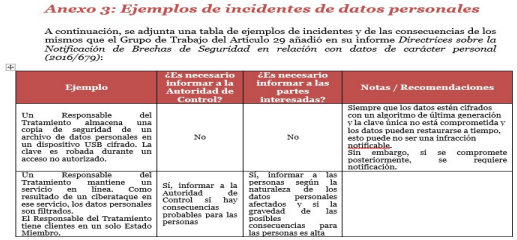
Procedimiento de brechas de seguridad:

Cuándo se descubra una brecha de seguridad los empleados del Concesionario deberán actuar conforme a lo establecido en el Protocolo de Respuesta ante incidentes de seguridad.

- **Notificación a la AEPD:** se deberá notificar a la AEPD cualquier brecha de seguridad en el plazo máximo de **72 horas** después de que haya tenido constancia de ella, a menos que sea poco probable que dicha violación constituya un riesgo para los derechos de los interesados.

- **Comunicación a los interesados:** cuando la brecha de seguridad conlleve un alto riesgo para los derechos y libertades de los interesados.

- **Documentación de la brecha:** Toda brecha debe ser documentada. Para ello, el Concesionario cuenta con una Plantilla de Gestión de Incidentes de Seguridad.



Anexo 3: Ejemplos de incidentes de datos personales

A continuación, se adjunta una tabla de ejemplos de incidentes y de las consecuencias de los mismos que el Grupo de Trabajo del Artículo 29 añadió en su informe *Directrices sobre la Notificación de Brechas de Seguridad en relación con datos de carácter personal (2016/679)*:

Ejemplo	¿Es necesario informar a la Autoridad de Control?	¿Es necesario informar a las partes interesadas?	Notas / Recomendaciones
Un Responsable del Tratamiento almacena una copia de seguridad de un archivo de datos personales en un dispositivo USB cifrado. La clave es robada durante un acceso no autorizado.	No	No	Siempre que los datos estén cifrados con un algoritmo de última generación y la clave única no está comprometida y los datos pueden restaurarse a tiempo, esto puede no ser una infracción notificable. Sin embargo, si se compromete posteriormente, se requiere notificación.
Un Responsable del Tratamiento mantiene un servicio en línea. Como resultado de un ciberataque en ese servicio, los datos personales son filtrados. El Responsable del Tratamiento tiene clientes en un solo Estado Miembro.	Sí, informar a la Autoridad de Control si hay consecuencias probables para las personas	Sí, informar a las personas según la naturaleza de los datos personales afectados y si la gravedad de las posibles consecuencias para las personas es alta	

Listado ejemplificativo de los diferentes tipos de incidentes que se pueden dar.

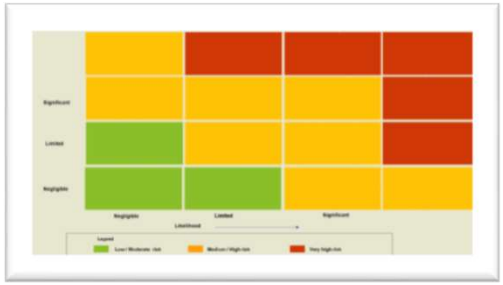
4.2. Metodología de adecuación al RGPD (iii)

Mapa de tratamientos:

Es importante recalcar que el registro de actividades de tratamiento es un documento vivo, en este sentido, el Concesionario tiene que actualizarlo cuando se modifiquen los tratamientos e incluir todos aquellos nuevos tratamientos que se realicen.

Valoración del riesgo:

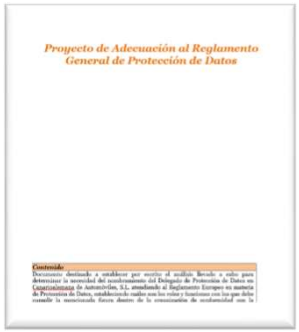
Cada vez que se lance un nuevo proyecto habrá que realizar una evaluación objetiva de impacto por cada tratamiento que implique el proyecto, en dicha evaluación se valora el riesgo que suponen tales tratamientos.



4.2. Metodología de adecuación al RGPD (iv)

Derechos ARCO+:

El Concesionario dispone de un protocolo para atender y dar respuesta a las solicitudes de ejercicio de alguno de los derechos ARCO+ que pueda recibir de los interesados.


Proyecto de Adecuación al Reglamento General de Protección de Datos

Protocolo de conservación:

El Concesionario debe mantener los datos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para la persecución de los fines del tratamiento de los datos personales.

Transcurrido dicho periodo, el Concesionario deberá proceder a la supresión de los mismos.

Gracias