TECNOSECURITY CONSULTING

CONSULTORÍA ESPECIALIZADA EN PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Socios corporativos

1.INTRODUCCIÓN

La protección de las personas físicas en relación con el tratamiento de datos personas es un derecho fundamental. El artículo 8, apartado 1 de la Carta de los Derechos Fundamentales de la Unión Europea ("la Carta") y el artículo 16, apartado 1 del Tratado de funcionamiento de la Unión Europea (TFUE) establecen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernen.

Para que el tratamiento sea licito, los datos personales deben ser tratados con el consentimiento del interesado o sobre alguna base legítima establecida conforme a Derecho, ya sea en el presente Reglamento o en virtud de otro Derecho de la Unión o de los Estados miembros a que se refiere el presente Reglamento, incluida la necesidad de cumplir la obligación legal aplicable al Responsable del tratamiento o la necesidad de ejecutar un contrato en el que sea parte el interesado o con objeto de tomar medidas a instancia del interesado o con objeto de tomar medidas a instancia del interesado con anterioridad a la conclusión de un contrato

En la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter personal (en lo sucesivo LOPD) tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

Por su parte, el Real Decreto 1720/2007 de Reglamento de Desarrollo de la LOPD nace con la necesidad de dotar de coherencia a la regulación reglamentaria existente hasta el momento y de desarrollar los aspectos novedosos de la LOPD, junto con aquellos en los que la experiencia ha aconsejado un cierto de grado de precisión que dote de seguridad jurídica al sistema.

El Reglamento tiene por objeto determinar y concretar las medidas jurídicas, técnicas y organizativas fijadas en el nuevo RGPD, en sus distintos niveles de seguridad, que son de obligado cumplimiento para todos aquellos autónomos y empresas que realicen cualquier tipo de tratamiento sobre datos de carácter personal.

Así mismo y de acuerdo con lo establecido en la RGPD, y en su normativa de desarrollo, procedemos a exponer el plan detallado de actuaciones que se

considera preciso llevar a cabo, para regularizar la situación de **----------.** así como la contraprestación económica que implica.

TECNOSECURITY, es una Consultoría Especializada en la adaptación y cumplimiento de la Ley y Reglamento Europeo de Protección de datos, con cobertura nacional y con servicio jurídico integral, garantizando un servicio totalmente personalizado.

Desde **TECNOSECURITY** consideramos de gran importancia la formación de cada uno de nuestros consultores para ofrecer un servicio de consultoría de máxima calidad. Igualmente, nuestro departamento jurídico ofrece el respaldo necesario de back-up al equipo de consultores y nos permite ofrecer adaptaciones presenciales, gracias a nuestro servicio de Adaptación Asistida in situ.

En definitiva, el principal beneficio que obtienen nuestros clientes, es la seguridad de encontrarse correctamente adaptado a la normativa vigente en la materia, estando protegido y respaldado, por una entidad líder en el sector, ante posibles sanciones derivadas de denuncias y/o inspecciones de la Agencia Española de Protección de Datos.

TECNOSECURITY cubre la totalidad de las necesidades en materia de protección de datos.

3.CONSULTORÍA Protección de Datos

Como especialistas en la implementación de la Protección de Datos, adaptamos nuestro servicio de consultoría a cualquier empresa o entidad jurídica mediante las siguientes fases:

Diagnosis Inicial

La primera fase para una correcta adaptación a la LOPD, consiste en la recogida de información relativa a la situación actual de la empresa con referencia al cumplimiento de lo dictado por la LOPD y nuevo RGPD, así como la identificación de la tipología de datos de carácter personal tratados. La importancia de cumplimentar toda la información de cada uno de los apartados es fundamental para poder llevar a cabo correctamente las siguientes fases de la adaptación

"Qué tipo de datos de carácter personal se manejan y cómo se tratan"

Deber de información

El deber de información a las personas de las cuales se vaya a obtener cualquier tipo de datos personales, previo al tratamiento de sus datos de carácter personal, es uno de los principios fundamentales sobre los que se asienta la LOPD y así viene encuadrado dentro de su Título II.

Este principio es, a la vez que una obligación para los responsables de los tratamientos, un derecho de los titulares de los datos y, muchas veces, constituye la primera ayuda que tiene el ciudadano para poder ejercitar el resto de derechos que marca la Ley (Acceso, Rectificación, Cancelación y Oposición).

El artículo 5 de la LOPD señala lo siguiente:

1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

> a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
>
> b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.
>
> c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
>
> d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
>
> e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante. Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de tránsito, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.

3. No será necesaria la información a que se refieren las letras b), c) y d) del apartado 1 (uno), si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.

4. Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presente artículo.

5. No será de aplicación lo dispuesto en el apartado anterior cuando expresamente una Ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia Española de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias.

Asimismo, tampoco regirá lo dispuesto en el apartado anterior cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento, así como de los derechos que le asisten".

Por tanto, cada persona de la que se pretenda recabar sus datos personales deberá ser informada previamente de todo el contenido del artículo 5.1 para que así conozca para qué finalidad se van a tratar, y por quién, pudiendo además en cualquier momento ejercitar sus derechos de acceso, rectificación, cancelación u oposición.

Si la recogida de los datos se ha realizado sin el conocimiento del interesado se le deberá de informar en el plazo de los tres meses siguientes al tratamiento, del contenido de cada uno de los puntos del artículo 5.1, quedando únicamente exceptuados de esta información aquellos supuestos en que una ley expresamente así lo establezca, o cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados a criterio de esta Agencia.

A este respecto, el artículo 19 del RLOPD recoge los siguientes supuestos especiales:

"En los supuestos en los que se produzca una modificación del responsable del fichero como consecuencia de una operación de fusión, escisión, cesión global de activos y pasivos, aportación o transmisión de negocio o rama de actividad empresarial, o cualquier operación de reestructuración societaria de análoga naturaleza, contemplada por la legislación mercantil, no se producirá cesión de datos, sin perjuicio del cumplimiento por el responsable de lo dispuesto en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre".

El incumplimiento del deber de información que contiene el precepto transcrito se encuentra tipificado como falta leve en el artículo 44.2.d) de la Ley Orgánica 15/1999: "El incumplimiento del deber de información al afectado acerca del tratamiento de sus datos de carácter personal cuando los datos sean recabados del propio interesado" y como falta grave en el artículo 44.3.c): "El incumplimiento del deber de información al afectado acerca del tratamiento de sus datos de carácter personal cuando los datos no hayan sido recabados del propio interesado".

Tratamiento

El artículo 5.1.t) del RLOPD define al tratamiento de datos como "cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias".

Como regla general, la inclusión de datos de carácter personal en un fichero supondrá un tratamiento de datos de carácter personal, que requerirá, en principio, el consentimiento del afectado.

"Artículo 6. Consentimiento del afectado".

1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa.

2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocio, laboral o administrativa y sean necesarios para

su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.

4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una Ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado".

En cuanto al consentimiento, el artículo 3.h) de la Ley Orgánica 15/1999 lo define como tal "toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen". De ello se desprende la necesaria concurrencia para que el consentimiento pueda ser considerado conforme a derecho de los cuatro requisitos enumerados en dicho precepto.

A juicio de esta Agencia la interpretación que ha de darse a estas cuatro notas características del consentimiento, siguiendo a tal efecto los criterios sentados en las diversas recomendaciones emitidas por el Comité de Ministros del Consejo de Europa, será las siguientes:

- **Libre**, lo que supone que el mismo deberá haber sido obtenido sin la intervención de vicio alguno del consentimiento en los términos regulados por el Código Civil.
- **Específico**, es decir, referido a una determinada operación de tratamiento y para una finalidad determinada, explícita y legítima del responsable del tratamiento, tal y como impone el artículo 4.2 de la LOPD.
- **Informado**, es decir que el afectado conozca con anterioridad al tratamiento la existencia del mismo y las finalidades para las que el

mismo se produce. Precisamente por ello el artículo 5.1 de la LOPD impone el deber de informar a los interesados de una serie de extremos que en el mismo se contienen.

- **Inequívoco**, lo que implica que no resulta admisible deducir el consentimiento de los meros actos realizados por el afectado (consentimiento presunto), siendo preciso que exista expresamente una acción u omisión que implique la existencia del consentimiento.

De lo que se ha indicado se desprende que de las características del consentimiento no se infiere necesariamente su carácter expreso en todo caso, razón por la cual en aquellos supuestos en que el legislador ha pretendido que el consentimiento deba revestir ese carácter, lo ha indicado expresamente; así sucede en el caso de tratamiento de datos especialmente protegidos, indicando el artículo 7.2 la necesidad de consentimiento expreso y escrito para el tratamiento de los datos de ideología, religión, creencias y afiliación sindical, y el artículo 7.3 la necesidad de consentimiento expreso aunque no necesariamente escrito para el tratamiento de los datos relacionados con la salud, el origen racial y la vida sexual.

Por tanto, el consentimiento podrá ser tácito, en el tratamiento de datos que no sean especialmente protegidos (artículo 7.2 y 7.3 de la Ley Orgánica 15/1999) si bien para que ese consentimiento tácito pueda ser considerado inequívoco será preciso otorgar al afectado un plazo prudencial para que pueda claramente tener conocimiento de que su omisión de oponerse al tratamiento implica un consentimiento al mismo, no existiendo al propio tiempo duda alguna de que el interesado ha tenido conocimiento de la existencia del tratamiento y de la existencia de ese plazo para evitar que se proceda al mismo.

El tratamiento de datos sin consentimiento previo del afectado en aquellos supuestos no exceptuados legalmente, puede ser motivo de infracción grave de acuerdo con lo dispuesto en el artículo 44.3.b) de la Ley Orgánica 15/1999.

Deber de guardar secreto.

El artículo 10 de la Ley Orgánica 15/1999 exige a quienes intervengan en cualquier fase del tratamiento de los datos, en el amplio sentido en que lo define el artículo 3, c), guardar secreto profesional sobre los datos, subsistiendo la obligación aun después de finalizar su relación con el responsable del fichero.

"Artículo 10. Deber de secreto".

El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo".

El incumplimiento del deber de secreto constituye infracción grave de acuerdo con lo previsto en el artículo 44.3.d) de la LOPD: "La vulneración del deber de guardar secreto acerca del tratamiento de los datos de carácter personal al que se refiere el artículo 10 de la presente Ley".

El Reglamento de protección de datos en 12 preguntas

El Reglamento General de Protección de Datos ha entrado en vigor el 25 de mayo de 2016. La AEPD ha elaborado este documento simplificado, que sigue el formato pregunta-respuesta, para facilitar la comprensión del nuevo marco normativo a los ciudadanos y ayudar a las organizaciones a adaptarse a los cambios que incorpora y cumplir así con sus obligaciones.

1. ***La entrada en vigor del Reglamento, ¿supone que ya no se aplica la Ley Orgánica de Protección de Datos española***

   No. El Reglamento ha entrado en vigor el 25 de mayo de 2016 pero no comenzará a aplicarse hasta, el 25 de mayo de 2018. Hasta entonces, tanto la Directiva 95/46 como las normas nacionales que la trasponen, entre ellas la española, siguen siendo plenamente válidas y aplicables.

2. ***¿Cuál es, entonces, el significado de que el Reglamento haya entrado en vigor?***

   El periodo de dos años hasta la aplicación del Reglamento tiene como objetivo permitir que los Estados de la Unión Europea, las Instituciones Europeas y también las organizaciones que tratan datos vayan preparándose y adaptándose para el momento en que el Reglamento sea aplicable.

   En esos dos años, por ejemplo, los Estados miembros pueden adoptar o iniciar la elaboración de determinadas normas que sean necesarias para permitir o facilitar la aplicación del Reglamento. Esas normas no pueden ser contrarias a las disposiciones de la vigente Directiva ni tampoco ir más allá

de los poderes de actuación normativa que el propio Reglamento prevé de forma explícita o implícita.

3. ***¿A qué empresas u organizaciones se aplica?***

   El Reglamento se aplicará como hasta ahora a responsables o encargados de tratamiento de datos establecidos en la Unión Europea, y se amplía a responsables y encargados no establecidos en la UE siempre que realicen tratamientos derivados de una oferta de bienes o servicios destinados a ciudadanos de la Unión o como consecuencia de una monitorización y seguimiento de su comportamiento.

   Para que esta ampliación del ámbito de aplicación pueda hacerse efectiva, esas organizaciones deberán nombrar un representante en la Unión Europea, que actuará como punto de contacto de las Autoridades de supervisión y de los ciudadanos y que, en caso necesario, podrá ser destinatario de las acciones de supervisión que desarrollen esas autoridades. Los datos de contacto de ese representante en la Unión deberán proporcionarse a los interesados entre la información relativa a los tratamientos de sus datos personales.

4. ***¿Qué implica para los ciudadanos que el Reglamento amplíe el ámbito de aplicación territorial?***

   Esta novedad supone una garantía adicional a los ciudadanos europeos. En la actualidad, para tratar datos no es necesario mantener una presencia física sobre un territorio, por lo que el Reglamento pretende adaptar los criterios que determinan qué empresas deben cumplirlo a la realidad del mundo de internet.

   Ello permite que el Reglamento sea aplicable a empresas que, hasta ahora, podían estar tratando datos de personas en la Unión y, sin embargo, se regían por normativas de otras regiones o países que no siempre ofrecen el mismo nivel de protección que la normativa europea.

5. ***¿Qué nuevas herramientas de control de sus datos poseen los ciudadanos?***

   El Reglamento introduce nuevos elementos, como el derecho al olvido y el derecho a la portabilidad, que mejoran la capacidad de decisión y control de los ciudadanos sobre los datos personales que confían a terceros.

   El derecho al olvido se presenta como la consecuencia del derecho que tienen los ciudadanos a solicitar, y obtener de los responsables, que los datos personales sean suprimidos cuando, entre otros casos, estos ya no sean necesarios para la finalidad con la que fueron recogidos, cuando se haya retirado el consentimiento o cuando estos se hayan recogido de forma ilícita. Asimismo, según la sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014, que reconoció por primera vez el derecho al olvido recogido ahora en el Reglamento europeo, supone que el interesado puede solicitar que se bloqueen en las listas de resultados de los buscadores los vínculos que conduzcan a informaciones que le afecten que resulten obsoletas, incompletas, falsas o irrelevantes y no sean de interés público, entre otros motivos.

Por su parte, el derecho a la portabilidad implica que el interesado que haya proporcionado sus datos a un responsable que los esté tratando de modo automatizado podrá solicitar recuperar esos datos en un formato que le permita su traslado a otro responsable. Cuando ello sea técnicamente posible, el responsable deberá trasferir los datos directamente al nuevo responsable designado por el interesado.

6. ***¿A qué edad pueden los menores prestar su consentimiento para el tratamiento de sus datos personales?***

   El Reglamento establece que la edad en la que los menores pueden prestar por sí mismos su consentimiento para el tratamiento de sus datos personales en el ámbito de los servicios de la sociedad de la información (por ejemplo, redes sociales) es de 16 años. Sin embargo, permite rebajar esa edad y que cada Estado miembro establezca la suya propia, estableciendo un límite inferior de 13 años. En el caso de España, ese límite continúa en 14 años. Por debajo de esa edad, es necesario el consentimiento de padres o tutores. En el caso de las empresas que recopilen datos personales, es importante recordar que el consentimiento tiene que ser verificable y que el aviso de privacidad debe estar escrito en un lenguaje que los niños puedan entender.

7. ***¿Qué implica la responsabilidad activa recogida en el Reglamento?***

   Uno de los aspectos esenciales del Reglamento es que se basa en la prevención por parte de las organizaciones que tratan datos. Es lo que se conoce como responsabilidad activa. Las empresas deben adoptar medidas que aseguren razonablemente que están en condiciones de cumplir con los principios, derechos y garantías que el Reglamento establece. El Reglamento entiende que actuar sólo cuando ya se ha producido una infracción es insuficiente como estrategia, dado que esa infracción puede causar daños a los interesados que pueden ser muy difíciles de compensar o reparar. Para ello, el Reglamento prevé una batería completa de medidas:

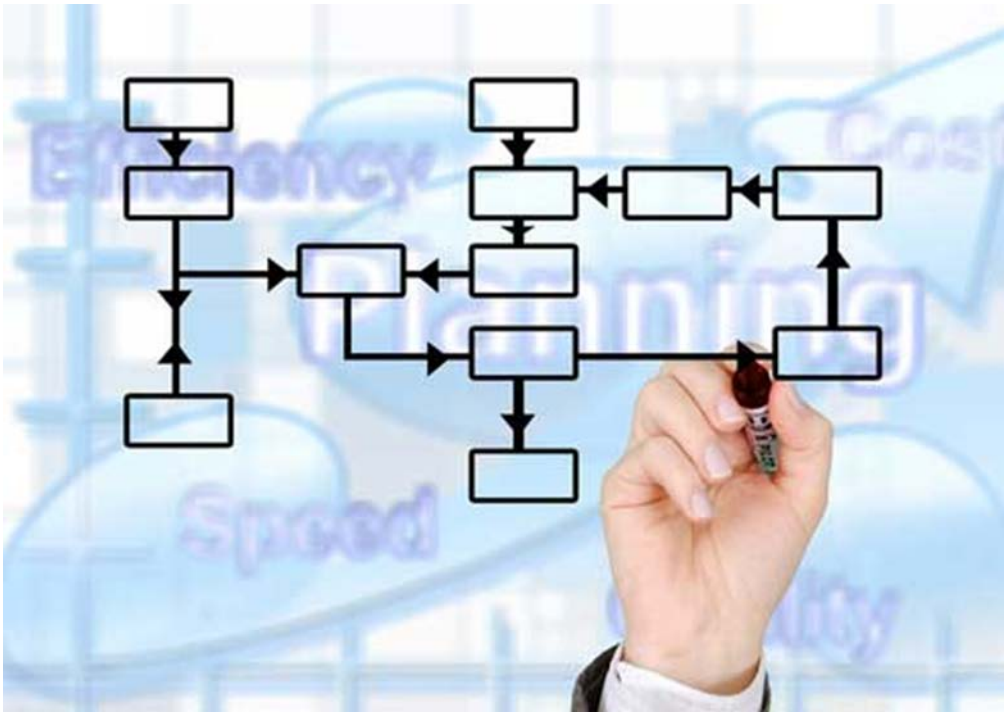
- Protección de datos desde el diseño
- Protección de datos por defecto
- Medidas de seguridad
- Mantenimiento de un registro de tratamientos
- Realización de evaluaciones de impacto sobre la protección de datos
- Nombramiento de un delegado de protección de datos
- Notificación de violaciones de la seguridad de los datos
- Promoción de códigos de conducta y esquemas de certificación.

8. ***Entonces, ¿supone una mayor carga de obligaciones para las empresas?***

El Reglamento supone un mayor compromiso de las organizaciones, públicas o privadas, con la protección de datos. Pero ello no implica necesariamente ni en todos los casos una mayor carga. En muchos casos será sólo una forma de gestionar la protección de datos distinta de la que se viene empleando ahora.

En primer lugar, algunas de las medidas que introduce el Reglamento son una continuación o reemplazan a otras ya existentes, como es el caso de las medidas de seguridad o de la obligación de documentación y, hasta cierto punto, la evaluación de impacto y la consulta a Autoridades de supervisión.

Otras constituyen la formalización en una norma legal de prácticas ya muy extendidas en las empresas o que, en todo caso, formarían parte de una correcta puesta en marcha de un tratamiento de datos, como pueden ser la privacidad desde el diseño y por defecto, la evaluación de impacto sobre protección de datos en ciertos casos o la existencia de un delegado de protección de datos.



En todos los casos, el Reglamento prevé que la obligación de estas medidas, o el modo en que se apliquen, dependerá de factores tales como el tipo de tratamiento, los costes de implantación de las medidas o el riesgo que el tratamiento presenta para los derechos y libertades de los titulares de los datos.

Por ello, es necesario que todas las organizaciones que tratan datos realicen un análisis de riesgo de sus tratamientos para poder determinar qué medidas han de aplicar y cómo hacerlo. Estos análisis pueden ser operaciones muy simples en entidades que no llevan a cabo más que unos pocos tratamientos sencillos que no impliquen, por ejemplo, datos sensibles, u operaciones más complejas en entidades que desarrollen muchos tratamientos, que afecten a gran cantidad de interesados o que por sus características requieren de una valoración cuidadosa de sus riesgos.

Las Autoridades de protección de datos europeas de forma colectiva, y la Agencia Española individualmente, estamos ya trabajando en el desarrollo de herramientas que faciliten la identificación y valoración de riesgos y en recomendaciones sobre la aplicación de medidas, especialmente en relación

con pymes que realizan los tratamientos de datos más habituales en la gestión empresarial.

9. ¿Cambia la forma en la que hay que obtener el consentimiento?

Una de las bases fundamentales para tratar datos personales es el consentimiento. El Reglamento pide que el consentimiento, con carácter general, sea libre, informado, específico e inequívoco. Para poder considerar que el consentimiento es ¿inequívoco?, el Reglamento requiere que haya una declaración de los interesados o una acción positiva que indique el acuerdo del interesado. El consentimiento no puede deducirse del silencio o de la inacción de los ciudadanos.

Las empresas deberían revisar la forma en la que obtienen y registran el consentimiento. Prácticas que se encuadran en el llamado consentimiento tácito y que son aceptadas bajo la actual normativa dejarán de serlo cuando el Reglamento sea de aplicación.

Además, el Reglamento prevé que el consentimiento haya de ser ¿explícito? en algunos casos, como puede ser para autorizar el tratamiento de datos sensibles. Se trata de un requisito más estricto, ya que el consentimiento no podrá entenderse como concedido implícitamente mediante algún tipo de acción positiva. Así, será preciso que la declaración u acción se refieran explícitamente al consentimiento y al tratamiento en cuestión.

Hay que tener en cuenta que el consentimiento tiene que ser verificable y que quienes recopilen datos personales deben ser capaces de demostrar que el

afectado les otorgó su consentimiento. Por ello, es importante revisar los sistemas de registro del consentimiento para que sea posible verificarlo ante una auditoría.

10. ¿Deben las empresas revisar sus avisos de privacidad?

Con carácter general, sí. El Reglamento prevé que se incluyan en la información que se proporciona a los interesados una serie de cuestiones que con la Directiva y muchas leyes nacionales de trasposición no eran necesariamente obligatorias. Por ejemplo, habrá que explicar la base legal para el tratamiento de los datos, los períodos de retención de los mismos y que los interesados puede dirigir sus reclamaciones a las Autoridades de protección de datos. Si creen que hay un problema con la forma en que están manejando sus datos. Es importante recordar que el Reglamento exige de forma expresa que la información que se proporcione sea fácil de entender y presentarse en un lenguaje claro y conciso.

11. ¿En qué consiste el sistema de 'ventanilla única'?

Este sistema está pensado para que los responsables establecidos en varios Estados miembros o que, estando en un solo Estado miembro, hagan tratamientos que afecten significativamente a ciudadanos en varios Estados de la UE tengan una única Autoridad de protección de datos como interlocutora. También implica que cada Autoridad de protección de datos europea, en lugar de analizar una denuncia o autorizar un tratamiento a nivel estrictamente nacional, a partir de la aplicación del Reglamento valorará si el supuesto tiene carácter transfronterizo, en cuyo caso habrá que abrir un procedimiento de cooperación entre todas las Autoridades afectadas buscando una solución aceptable para todas ellas. Si hay discrepancias insalvables, el caso puede elevarse al Comité Europeo de Protección de Datos, un organismo de la Unión integrado por los directores de todas las Autoridades de protección de datos de la Unión. Ese Comité resolverá la controversia mediante decisiones vinculantes para las Autoridades implicadas.

Este nuevo sistema no supone que los ciudadanos tengan que relacionarse con varias Autoridades o con Autoridades distintas de la del Estado donde residan. Siempre pueden plantear sus reclamaciones o denuncias ante su propia Autoridad nacional (en el caso español, la Agencia Española de Protección de Datos). La gestión será realizada por esa Autoridad, que será también

responsable de informar al interesado del resultado final de su reclamación o denuncia.

La ventanilla única, en todo caso, no afectará a empresas que sólo estén en un Estado miembro y que realicen tratamientos que afecten sólo a interesados en ese Estado.

12. ***¿Tienen las empresas que empezar a aplicar ya las medidas contempladas en el Reglamento?***

No. El Reglamento está en vigor, pero no será aplicable hasta 2018.

Sin embargo, puede ser útil para las organizaciones que tratan datos empezar ya a valorar la implantación de algunas de las medidas previstas, siempre que esas medidas no sean contradictorias con las disposiciones de la LOPD, que sigue siendo la norma por la que han de regirse los tratamientos de datos en España.

Por ejemplo, las organizaciones deben tener en cuenta que a partir de mayo de 2018 deberán realizar análisis de riesgo de sus tratamientos y que puede ser útil para ellas empezar desde ahora a identificar el tipo de tratamientos que realizan, el grado de complejidad del análisis que deberán llevar a cabo, etc. En esta tarea podrían utilizar las herramientas y recursos que paulatinamente vayan desarrollando las Autoridades de protección de datos.

Igualmente, nada impide que las organizaciones comiencen a planificar o a establecer el registro de tratamientos de datos o a implantar las evaluaciones de impacto o cualquiera otra de las medidas previstas.

Del mismo modo, las organizaciones podrían comenzar a diseñar e implantar los procedimientos para notificar adecuadamente a las Autoridades de protección de datos o a los interesados las quiebras de seguridad que pudieran producirse.

En general, las organizaciones que tratan datos personales deberían comenzar a preparar la aplicación de estas medidas, así como de otras modificaciones prácticas derivadas del Reglamento. Por ejemplo, el Reglamento exige que los responsables de tratamiento faciliten a los interesados el ejercicio de sus derechos. Aunque la interpretación de ¿facilitar? pueda variar dependiendo de los casos, incluye en todos ellos algún tipo de actuación positiva por parte de los

responsables para hacer más accesibles y sencillas las vías para el ejercicio de derechos.

La ventaja de una pronta aplicación es que permitirá detectar dificultades, insuficiencias o errores en una etapa en que estas medidas no son obligatorias y, en consecuencia, su corrección o eficacia no estarían sometidas a supervisión. Ello permitiría corregir errores para el momento en que el Reglamento sea de aplicación.

Notificación de ficheros

De acuerdo con la información recogida en la fase anterior, **TECNOSECURITY** notifica las altas, modificaciones o supresiones de los ficheros, de **----------**, al Registro General de la Agencia Española de Protección de Datos en cumplimiento de lo establecido en la LOPD y prestando especial atención a la finalidad del tratamiento de los ficheros identificados.

Documento de Seguridad

Según la obligación establecida en el artículo 88 del Reglamento de desarrollo de la LOPD aprobado por el Real Decreto 1720/2007, de 21 de diciembre, todas las entidades jurídicas deben contar con un Documento de Seguridad en el que se regulen las medidas de seguridad de los ficheros, automatizados o no, que contengan datos de carácter personal. **TECNOSECURITY** elabora un Documento de Seguridad personalizado a **----------**de acuerdo con la información recogida en la fase de Diagnosis Inicial y de conformidad con lo estipulado en el Reglamento de desarrollo de la LOPD.

Textos y Contratos Jurídicos

De acuerdo con las necesidades de **----------** detectadas durante el proyecto, **TECNOSECURITY** elabora un documento personalizado llamado "Textos Jurídicos" que incluye:

- **Cláusulas informativas y de consentimiento** para el tratamiento y la cesión
- **Cláusulas** y **Carteles** Homologados para la regulación de Sistemas de Videovigilancia
- **Contrato de tratamiento por cuenta de terceros a formalizar por los Encargados de Tratamiento.**

- **Manual de Funciones y Obligaciones** del personal, así como Compromiso de Confidencialidad para los empleados.

Informe Web

TECNOSECURITY personaliza un Informe Web que contiene los textos que se deben incluir en sus páginas web, en cumplimiento de la normativa en materia de protección de datos y de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI-CE)

Adaptación Asistida

La gerencia de **TECNOSECURITY** realiza la presentación de toda la documentación y ofrece el apoyo necesario para verificar la correcta implementación de las medidas de seguridad.

Auditorias de control

TECNOSECURITY con el objeto de verificación establecida en el RGPD, facilitará trimestralmente un cuestionario que incluirá los aspectos a verificar y/o modificar, manteniendo actualizada la adaptación de su empresa y nuestro Certificado.

Certificado RGPD

Garantizando que se han llevado a cabo los puntos anteriormente citados, **TECNOSECURITY** certifica que cumple con la Normativa en materia de Protección de Datos.

Asesoramiento Jurídico

TECNOSECURITY proporciona asesoramiento jurídico ilimitado en materia de protección de datos, a todos sus clientes a través de sus **abogados expertos en Protección de Datos**.

Seguro de Responsabilidad Civil

TECNOSECURITY dispone de un seguro de responsabilidad civil que cubre la totalidad de sus actuaciones en materia de protección de datos. Este seguro proporciona una cobertura total de hasta 300.000 € por cliente de las actuaciones derivadas de **TECNOSECURITY** para posibles expedientes sancionadores.

Artículo 28 de RGPD:

1. Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado.
2. El encargado del tratamiento no recurrirá a otro encargado sin la autorización previa por escrito, específica o general, del responsable. En este último caso, el encargado informará al responsable de cualquier cambio previsto en la incorporación o sustitución de otros encargados, dando así al responsable la oportunidad de oponerse a dichos cambios.
3. El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto al responsable y establezca 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. Dicho contrato o acto jurídico estipulara que el encargado:

a) Tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público;
b) Garantizara que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad
c) Tomará todas las medidas necesarias de conformidad con el articulo 32
d) Respetará las condiciones indicadas en los apartados 2 y 4 para recurrir a otro encargado del tratamiento;
e) asistirá al responsable, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las

solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III;

f) Ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado;

g) A elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros;

h) Pondrá 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, por parte del responsable o de otro auditor autorizado por dicho responsable. 4.5.2016 ES Diario Oficial de la Unión Europea L 119/49

En relación con lo dispuesto en la letra h) del párrafo primero, el encargado informará inmediatamente al responsable si, en su opinión, una instrucción infringe el presente Reglamento u otras disposiciones en materia de protección de datos de la Unión o de los Estados miembros.

4. Cuando un encargado del tratamiento recurra a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se impondrán a este otro encargado, mediante contrato u otro acto jurídico establecido con arreglo al Derecho de la Unión o de los Estados miembros, las mismas obligaciones de protección de datos que las estipuladas en el contrato u otro acto jurídico entre el responsable y el encargado a que se refiere el apartado 3, en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones del presente Reglamento. Si ese otro encargado incumple sus obligaciones de protección de datos, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado.

5. La adhesión del encargado del tratamiento a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá utilizarse como elemento para demostrar la existencia de las garantías suficientes a que se refieren los apartados 1 y 4 del presente artículo.
6. Sin perjuicio de que el responsable y el encargado del tratamiento celebren un contrato individual, el contrato u otro acto jurídico a que se refieren los apartados 3 y 4 del presente artículo podrá basarse, total o parcialmente, en las cláusulas contractuales tipo a que se refieren los apartados 7 y 8 del presente artículo, inclusive cuando formen parte de una certificación concedida al responsable o encargado de conformidad con los artículos 42 y 43.
7. La Comisión podrá fijar cláusulas contractuales tipo para los asuntos a que se refieren los apartados 3 y 4 del presente artículo, de acuerdo con el procedimiento de examen a que se refiere el artículo 93, apartado 2.
8. Una autoridad de control podrá adoptar cláusulas contractuales tipo para los asuntos a que se refieren los apartados 3 y 4 del presente artículo, de acuerdo con el mecanismo de coherencia a que se refiere el artículo 63.
9. El contrato u otro acto jurídico a que se refieren los apartados 3 y 4 constará por escrito, inclusive en formato electrónico. 10. Sin perjuicio de lo dispuesto en los artículos 82, 83 y 84, si un encargado del tratamiento infringe el presente Reglamento al determinar los fines y medios del tratamiento, será considerado responsable del tratamiento con respecto a dicho tratamiento.

PERFIL DEL PUESTO DE DELEGADO DE PROTECCIÓN DE DATOS.

El DPD es un profesional cuyas funciones se señalan en el artículo 39 del Reglamento (UE) 679/2016, y se ocupa de la aplicación de la legislación sobre privacidad y protección de datos. El delegado de protección de datos tendrá como mínimo las siguientes funciones:

- informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;

- supervisar el cumplimiento de lo dispuesto en el Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales,
- supervisar la asignación de responsabilidades,
- supervisar la concienciación y formación del personal que participa en las operaciones de tratamiento
- supervisar las auditorías correspondientes;
- ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos
- supervisar su aplicación de conformidad con el artículo 35 del Reglamento;
- cooperar con la autoridad de control;
- actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36;
- realizar consultas a la autoridad de control, en su caso, sobre cualquier otro asunto.

El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

Para ello deberá ser capaz de:

a) recabar información para determinar las actividades de tratamiento,
b) analizar y comprobar la conformidad de las actividades de tratamiento, e
c) informar, asesorar y emitir recomendaciones al responsable o el encargado del tratamiento.
d) recabar información para supervisar el registro de las operaciones de tratamiento.
e) asesorar en la aplicación del principio de la protección de datos por diseño y por defecto.
   - asesorar sobre: si se debe llevar a cabo o no una evaluación de impacto de la protección de datos, qué metodología debe seguirse al efectuar una evaluación de impacto de la protección de datos, si se debe llevar a cabo

la evaluación de impacto de la protección de datos con recursos propios o con contratación externa.

- Qué salvaguardas (incluidas medidas técnicas y organizativas) aplicar para mitigar cualquier riesgo para los derechos e intereses de los afectados si se ha llevado a cabo correctamente o no la evaluación de impacto de la protección de datos y, si sus conclusiones (si seguir adelante o no con el tratamiento y qué salvaguardas aplicar) son conformes con el Reglamento.

f) priorizar sus actividades y centrar sus esfuerzos en aquellas cuestiones que presenten mayores riesgos relacionados con la protección de datos.

g) asesorar al responsable del tratamiento sobre:

- Metodologías a emplear al llevar a cabo una evaluación de impacto de la protección de datos, qué áreas deben someterse a auditoría de protección de datos interna o externa, qué actividades de formación internas proporcionar al personal o los directores responsables de las actividades de tratamiento de datos y a qué operaciones de tratamiento dedicar más tiempo y recursos.

COMPETENCIAS REQUERIDAS AL PUESTO DE DELEGADO DE PROTECCIÓN DE DATOS.

El DPD deberá reunir conocimientos especializados del Derecho y la práctica en materia de protección de datos. Se han identificado, en consecuencia, aquellos conocimientos, habilidades o destrezas necesarias que tiene que saber o poseer la persona a certificar para llevar a cabo cada una de las funciones propias del puesto de Delegado de Protección de Datos. Estas funciones genéricas del DPD se pueden concretar en tareas de asesoramiento y supervisión, entre otras, en las siguientes áreas:

1. Cumplimiento de principios relativos al tratamiento, como los de limitación de finalidad, minimización o exactitud de los datos
2. Identificación de las bases jurídicas de los tratamientos
3. Valoración de compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos

4. Determinación de la existencia de normativa sectorial que pueda determinar condiciones de tratamiento específicas distintas de las establecidas por la normativa general de protección de datos
5. Diseño e implantación de medidas de información a los afectados por los tratamientos de datos
6. Establecimiento de mecanismos de recepción y gestión de las solicitudes de ejercicio de derechos por parte de los interesados
7. Valoración de las solicitudes de ejercicio de derechos por parte de los interesados
8. Contratación de encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación responsable-encargado
9. Identificación de los instrumentos de transferencia internacional de datos adecuados a las necesidades y características de la organización y de las razones que justifiquen la transferencia
10. Diseño e implantación de políticas de protección de datos
11. Auditoría de protección de datos
12. Establecimiento y gestión de los registros de actividades de tratamiento
13. Análisis de riesgo de los tratamientos realizados
14. Implantación de las medidas de protección de datos desde el diseño y protección de datos por defecto adecuadas a los riesgos y naturaleza de los tratamientos
15. Implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos
16. Establecimiento de procedimientos de gestión de violaciones de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de los afectados y los procedimientos de notificación a las autoridades de supervisión y a los afectados
17. Determinación de la necesidad de realización de evaluaciones de impacto sobre la protección de datos
18. Realización de evaluaciones de impacto sobre la protección de datos
19. Relaciones con las autoridades de supervisión
20. Implantación de programas de formación y sensibilización del personal en materia de protección de datos.