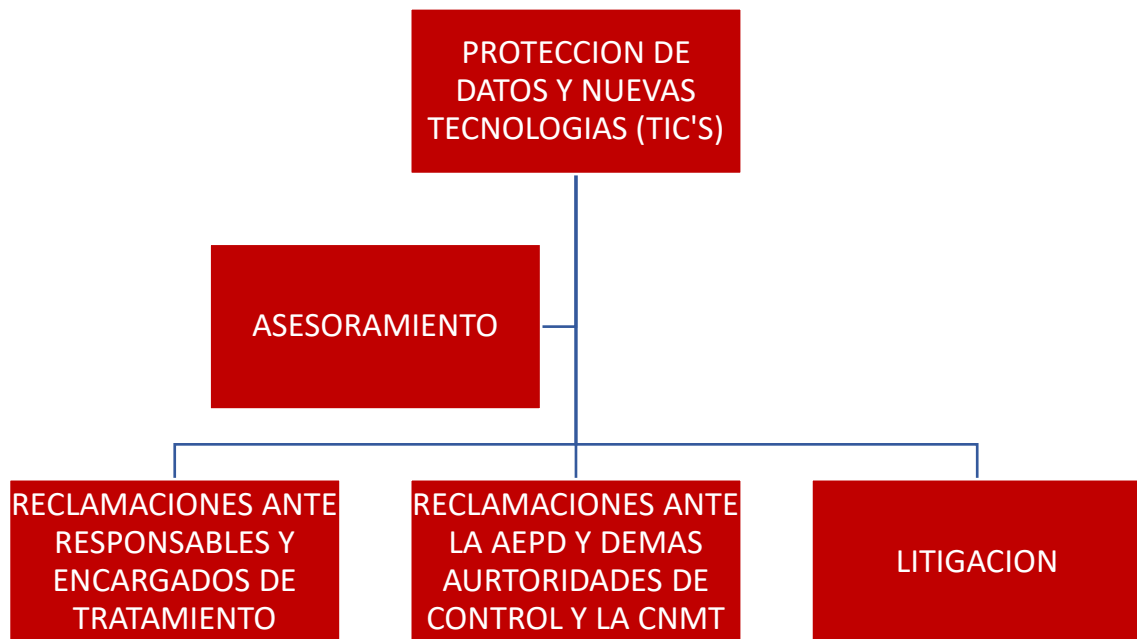


LA PROTECCION DE DATOS PERSONALES, Y LAS TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACIÓN (TIC'S)



Los datos de carácter personal son cualquier información referente a personas físicas identificadas o identificables, pudiendo ser identificable toda persona cuya identidad pueda determinarse mediante un identificador (por ejemplo, un nombre, un número de identificación, datos de localización o un identificador en línea) o mediante el uso de uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de las personas.

Dependiendo del tipo de datos que se traten, éstos pueden ser, por ejemplo, identificativos (nombre, apellidos, número del documento nacional de identidad), referidos a tu situación laboral, financiera o de salud.

También existen las categorías especiales de datos, en los que además de los datos de salud, se encuentran los que puedan revelar tu origen étnico o racial, opiniones políticas, convicciones religiosas o fisiológicas, o afiliación sindical, así como el tratamiento de tus datos genéticos, biométricos (si te identificasen de manera unívoca), así como los relativos a tu vida sexual u orientación sexual.

LOS PRINCIPIOS BÁSICOS

Como principio fundamental a conseguir con las medidas de protección de datos personales conviene y tener muy claro, lo siguiente:

“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”

El derecho fundamental que la protección de datos persigue garantizar y proteger es el tratamiento de los datos personales y los derechos fundamentales de las personas físicas; especialmente, el derecho al honor e intimidad personal y familiar.

Se reconoce a los ciudadanos la capacidad de controlar su propia información personal para que puedan tomar decisiones sobre ésta, como establecer quién puede utilizar su información personal, con qué finalidad, hasta cuándo y pudiendo acceder, limitar, rectificar u oponerse a esa posesión o uso, y ejercer todas las facultades de control al respecto.

Consecuentemente con ello, debe ser el propio ciudadano quien tiene la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como decidir sobre las finalidades con las que puede ser tratada su información y con quién puede ser compartida.

LOS CONCEPTOS BÁSICOS

Si bien no pretendo entrar a fondo en los conceptos legales vinculados con la protección de datos de carácter personal, sí es conveniente que les relacione una serie de conceptos que van a estar muy presentes a lo largo de esta serie de artículos:

- **Datos de carácter personal:** cualquier dato concerniente a personas físicas identificadas o identificables.
- **Fichero:** todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.
- **Tratamiento de datos:** Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

- **Responsable del fichero o tratamiento:** Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo que decida sobre la finalidad, contenido y uso del tratamiento.
- **Encargado del tratamiento:** Persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo, o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.
- **Responsable de seguridad:** persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordina y controlar las medidas de seguridad aplicables.
- **Afectado o interesado:** Persona física titular de los datos que sean objeto de tratamiento.
- **Persona identificable:** Toda persona cuya identidad pueda determinarse directa o indirectamente mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social.
- **Tercero:** La persona física o jurídica, pública o privada, u órgano administrativo distinta del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento.
- **Consentimiento del interesado:** Toda manifestación de voluntad libre, inequívoca, específica e informada mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.
- **Sistema de información:** Conjunto de ficheros, tratamientos, programas, soportes, y en su caso, equipos empleados para el tratamiento de datos de carácter personal.
- **Sistema de tratamiento:** Modo en que se organiza o utiliza un sistema de información. Atendiendo al sistema de tratamiento los sistemas de información podrán ser automatizados, no automatizados o parcialmente automatizados.
- **Copia de respaldo:** Copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.
- **Ficheros temporales:** Ficheros de trabajo creados por usuarios o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento.
- **Accesos autorizados:** Autorizaciones concedidas a un usuario para la utilización de los diversos recursos. En su caso incluirán las autorizaciones o funciones que tenga atribuidas un usuario por delegación del responsable del fichero o tratamiento o del responsable de seguridad.
- **Transferencia internacional de datos:** Tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español

¿ES LA PROTECCIÓN DE DATOS LA EXPRESIÓN DE UNA NUEVA CULTURA PARA LAS EMPRESAS Y LOS CIUDADANOS?

Tras la entrada en vigor del nuevo Reglamento 2016/679, se ha puesto más que nunca de manifiesto que la protección de datos de carácter personal entraña hoy por hoy, sobre todo una sólida cultura de cumplimiento, cada vez más arraigada entre los ciudadanos.

Es evidente que los tiempos cambian, y las modificaciones normativas producidas que ha introducido el citado Reglamento se encuentran íntimamente ligados y van en consonancia con el rápido desarrollo tecnológico producido en los últimos años, y la influencia que los mismos han tenido en la constitución de nuevas e influyentes prácticas sociales, lo que ha determinado a su vez, entre otras razones, esa necesidad de proceder a su actualización.

Consecuentemente con ello, la reforma legal producida, no debe ser solamente valorada como una cuestión de mera juridicidad, sino que tiene otras repercusiones muy trascendentes.

En este sentido, y tal como se ponía recientemente la gran **complejidad del Reglamento** es que no afecta a una única área de la organización sino que, de alguna manera, la atraviesa totalmente y **requiere un cambio cultural**.

Exige programas y **equipos cross-funcionales** trabajando en paralelo a través de múltiples líneas de negocio y geografías.

Desde los técnicos en sistemas IT, a los abogados de Compliance, pasando por los responsables de riesgos, de auditoría interna, de marketing y gestión de clientes (CRM)... y, por supuesto, de ciberseguridad. También deberán ir preparándose los departamentos de relación con clientes, inversores y medios de comunicación, que pronto tendrá para lidiar con este tipo de cuestiones.

Pero su puesta en marcha es, - sobre todo-, un punto de partida para **adoptar un nuevo enfoque en la cultura corporativa** hacia la **protección de datos**.

Así, se afirma que constituye “una cultura en la que la **transparencia**, los **derechos** de los ciudadanos y la **responsabilidad** sea algo automático y natural [...], de forma que todo el mundo en la organización **valore el derecho de los clientes a su privacidad**”.

Y que “sólo se podrá construir un entorno de confianza si las organizaciones contribuyen, con su **transparencia, responsabilidad y principios** a que los clientes sean conscientes de la información personal que éstas tienen de ellos y cómo los usan”.

De ahí que, que el ámbito de la privacidad hoy en día constituye una cultura que debe atender básicamente a situaciones muy precisas, pero que al mismo tiempo, son muy importantes desde una perspectiva estrictamente social, en las que se encuentran: el hecho de potenciar la educación y la cultura en la ciudadanía, específicamente en aras de proteger su privacidad en Internet y las redes sociales; la formación en el uso y alcance de la tecnología de tal manera que desaparezca o se reduzca lo más posible la brecha digital que cada día afecta a más ciudadanos en el ámbito de nuestras sociedades; la posibilidad de proporcionar una mayor información transparente y adecuada por parte de los prestadores de servicios a la ciudadanía; el establecimiento de medidas protectoras de la privacidad; y, finalmente, la atribución de mayores responsabilidades a los proveedores de servicios; así como la enseñanza y el desarrollo de un marco normativo que éste acorde en cada momento con los tiempos, especialmente con el avance tecnológico.

Todo ello refleja el hecho de que la cultura sobre la privacidad cada vez más tiene un marcado enfoque social, basada en las opiniones, las prácticas o las conductas asumidas socialmente por las personas, que viene a constituir un nuevo entorno de comunicación y de expresión, en la cual el individuo debe actuar siguiendo determinados patrones de conductas transmitidas socialmente, y que se basan primordialmente en los valores que se incluyen en la nueva normativa sobre privacidad.

Esta nueva cultura exige establecer una bases o criterios son determinantes para posibilitar la adaptación de los ciudadanos a este nuevo entorno normativo y social, y que, entre otros valores o principios, se pueden señalar los siguientes:

a). Es necesario partir de la existencia de unos mismos derechos y las obligaciones entre todas las personas que viven en el marco de nuestra sociedad. Ello constituye uno de los pilares básicos en los que se asienta el nuevo Reglamento Comunitario que apuesta por la igualdad de todos los ciudadanos que integran la misma, con independencia de cuál sea el lugar donde vivan o residan.

b) Este plano de igualdad sobre los derechos y obligaciones debe ser proyectado también sobre todos los operadores jurídicos que tratan datos de carácter personal.

En este sentido, constituye una obligación de todos dar cumplimiento a dichos valores, y poco o nada tendrían sentido, si los titulares de los datos reclaman el cumplimiento de la normativa vigente, y dichos operadores no se ajustan en sus tratamientos a la legalidad vigente.

c). Este panorama regulatorio, con impacto en la actividad cultural y social es imprescindible que encuentre una amplia y efectiva tutela entre las autoridades de control en el ámbito de la protección de datos de carácter personal, de modo y manera, que dicha supervisión sea coherente con los principios establecidos, y al mismo tiempo represente un impulso para la expansión de esta cultura de respeto a la privacidad de la persona, donde sea posible del todo punto compaginar dicha privacidad, con el crecimiento económico o la libre circulación de los datos personales.

Las empresas deben adecuarse a esta nueva normativa, pero los ciudadanos tienen que conocer sus derechos, y exigirlos, y hacerlos valer.

¿QUE SERVICIOS OFRECE PUYOL-ABOGADOS & PARTNERS?

En este ámbito de práctica profesional, PUYOL-ABOGADOS & PARTNERS ofrece los siguientes servicios de práctica profesional:

a). Para los ciudadanos:

- Defensa y tutela de sus derechos en materia de protección de datos y nuevas tecnologías.
- Ejercicio de derechos reconocidos en el RGPD y el LA LOPDGDD.
- Tutela de derechos ante la Agencia Española de Protección de Datos.
- Realización de denuncias por infracción de normativa ante dicha Agencia.
- Procedimientos judiciales en defensa de los derechos de los ciudadanos, y como consecuencia de las infracciones a la normativa cometidos por terceros, especialmente en lo que hace referencia al derecho al honor, a la intimidad personal y familiar y a la propia imagen.
- Ello, obviamente es extensivo a las acciones judiciales derivadas de la protección de datos personales.
- Solicitud de información a entidades públicas sobre la base de la Ley de Transparencia.

b). Para las empresas y demás personas jurídicas

La gestión de los ficheros y datos de las Empresas se lleva a cabo mediante la prestación de servicios de asesoría, consultoría y defensa jurídica integral en materia de protección de datos de carácter personal, abarca las siguientes funciones a título meramente enunciativo:

- Ejercicio de la función de Delegado de Protección de Datos (DPD/DPO)
- Desarrollo de las facultades de consultoría en su más amplia extensión
- Políticas de Privacidad, Avisos Legales, Políticas de Cookies, y Condiciones de uso de Páginas Webs
- COMERCIO ELECTRÓNICO (E-commerce), y regulaciones de BIG DATA, CLOUD COMPUTING, INTERNET DE LAS COSAS, BLOCKCHAIN, PROCESOS DE IDENTIFICACION Y AUTENTICACION, FIRMA ELECTRONICA, DESARROLLO JURIDICO DE APP'S, ETC.
- Aplicación completa del nuevo REGLAMENTO GENERAL (UE) 2016/679 DEL PROTECCION DE DATOS DE LA UNION EUROPEA, Y DE LA LEY ORGANICA 3/2015, DE 5 DE DICIEMBRE DE PROTECCION DE DATOS PERSONALES Y GARANTIA DE LOS DERECHOS DIGITALES a la empresa, y cumplimiento de las obligaciones que correspondan como responsable del fichero/tratamiento o como encargado de tratamiento
- Aplicación de la gestión territorial a todas las unidades y departamentos de la Empresa
- Gestión contractual y documental, incluidas páginas web, avisos legales, etc.
- Control jurídico en la materia en relación con los proveedores.
- La calificación jurídica legitimadora de los ficheros y tratamientos
- Información para elaborar el documento de seguridad, elaboración y explicación del mismo, o documentos análogos.

- **Determinación de los niveles y medidas de seguridad aplicables en cada caso.**
- **Gestión de los Derechos Arco y demás derechos contemplados en el Reglamento General de Protección de Datos.**
- **Adaptación a las modificaciones de la LOPD al REGLAMENTO GENERAL DE PROTECCION DE DATOS y demás normas jurídicas nacionales o europeas aplicables en la materia.**
- **Soporte jurídico ante inspecciones de AEPD.**
- **Gestión de reclamaciones de clientes y de terceros en la materia.**
- **Defensa jurídica integral ante cualquier situación precontenciosa o contenciosa derivada de la protección de datos de carácter personal (administrativa, civil, penal y contencioso/administrativa).**
- **Auditoria annual o bianual.**
- **Formación integral en materia de protección de datos de carácter personal a todos los empleados.**
- **Asesoramiento en la elaboración de proyectos con o sin necesidad de evaluación de impacto en materia de protección de datos.**
- **Asesoramiento y gestión jurídica ante la producción de brechas de seguridad.**
- **Gestión de transferencias internacionales de datos personales, Cláusulas Contractuales Tipo y BCR's.**
- **Formulación de consultas previas a la AEPD en los casos en que sea preceptivo de conformidad con el Reglamento General de Protección de Datos de la UE, y normativa que lo desarrolle.**
- **Elaboración de Código de Conducta y de Códigos-Tipo en protección de datos.**
- **Gestión para la obtención de certificaciones en materia de privacidad.**
- **Formación a los Gerentes, comerciales y a las personas vinculadas con la Empresa crea necesario que tengan conocimiento de la normativa sobre privacidad, al tener acceso a datos de carácter personal.**
- **Creación, estructuración y gestión de un órgano especializado en protección de datos y privacidad.**

- **Análisis de riesgos**
- **Análisis de la necesidad de realización de la Evaluación de Impacto**
- **Redacción de Formularios, políticas y otros instrumentos necesarios para el desenvolvimiento y aplicación de la protección de datos personales.**
- **Establecimiento y determinación de los perfiles laborales y profesionales de acceso a la información construida sobre los datos personales.**
- **Emisión de segundas opiniones en la implantación del GDPR y demás normativa de desarrollo, y en materia de auditoría.**
- **Formación específica adaptada a las necesidades de la empresa**
- **Intervención como experto independiente en los comités de prevención de privacidad y nuevas tecnologías.**
- **Cuanto otras prestaciones en materia de privacidad sean necesarias, derivadas de la entrada en vigor y efectiva aplicación del nuevo Reglamento General de Protección de datos de la Unión Europea o de la nueva Ley Orgánica de Protección de Datos.**
- **Solicitud de información a entidades públicas sobre la base de la Ley de Transparencia**