Alfonso Pacheco Cifuentes

gabinete jurídico y nuevas tecnologías

PRINCIPALES IMPLICACIONES DEL RGPD PARA UN DESPACHO DE ABOGADOS

OPORTUNIDAD DE NEGOCIO

Convenciones

- **AEPD** = Agencia Española de Protección de Datos
- **LOPD** = Ley Orgánica 15/1999, de 13 de diciembre de protección de datos personales
- **RDLOPD** = Real Decreto 1720/2007, de 21 de diciembre, Reglamento de desarrollo de la LOPD
- **RGPD** = Reglamento (UE) 2016/679 del Parlamento y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales.
- **LOPD 2.0** = proyecto nueva LOPD
  - Actualmente en el Congreso de los Diputados, proyecto 121/000013.
  - Serias dudas de aprobación y entrada en vigor antes del 25/5/2018

¿Debe un abogado cumplir con la normativa PD?

- El abogado **SI** accede a datos de carácter personal en el desarrollo de sus competencias.
- El abogado **SI** somete a esos datos de carácter personal a tratamiento informático y/o manual.
- ¿Para? Para el desarrollo de la prestación de servicios objeto de su contratación
- La ley se aplica a los datos de carácter personal registrados en un soporte físico **[AUTOMATIZADO O NO]** que los haga susceptibles de tratamiento, y a toda modalidad de uso por los sectores público y **privado** (artículo 2 LO 15/1999).
- El presente Reglamento se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero (artículo 2 RGPD 2016/679)
- **Por tanto, el abogado está obligado al cumplimiento del contenido de la normativa sobre protección de datos.**

Objetivo principal RGPD: CAFÉ PARA TODOS

El Reglamento general de protección de datos pretende con su eficacia directa superar los obstáculos que impidieron la finalidad armonizadora de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos. La transposición de la directiva por los Estados miembros se ha plasmado en un mosaico normativo con perfiles irregulares en el conjunto de la Unión Europea lo que, en último extremo, ha conducido a que existan diferencias apreciables en la protección de los derechos de los ciudadanos.

Ordenamiento Jurídico > PD

- El ordenamiento jurídico no es “eleopedecentrista”.
- Hay vida más allá de las normas sobre protección de datos.
- Necesidad de casar la PD con la normativa específica de aplicación en cada situación.

¿Vuelta a la casilla de salida?

- No partimos de cero.
- Hay trabajo hecho que no se tira a la basura, sino que se puede aprovechar.

¿Qué cambios trae el RGPD?

Entre otros, y siempre desde el punto de vista del despacho de abogado:

- Exigencia de una mayor conducta proactiva del responsable en el cumplimiento de los principios art. 5.
- Privacidad desde el diseño.
- Ampliación de las categorías de datos especialmente protegidos.
- Desaparición inscripción ficheros en la AEPD
- Ampliación de la información a facilitar a los interesados cuyos datos se vayan a tratar.
- Novedades en cuanto a la legitimación y consentimiento para el tratamiento de datos.
- Introducción de nuevos derechos de los interesados
- Introducción de la figura del Delegado de Protección de Datos.
- Introducción de los Análisis de Impacto en la Privacidad
- Nuevo régimen de medidas de seguridad.
- Nuevo régimen sancionador: de sanciones “bestias” a “muy bestias”.

Conducta proactiva

- Art. 5.2 RGPD

  El responsable del tratamiento será responsable del cumplimiento de los principios que deben regir todo tratamiento de datos personales y, además, debe ser capaz de demostrarlo.

¿Qué principios son esos? Los que establece el art. 5.1 RGPD

Principios básicos del tratamiento

- Licitud, lealtad y transparencia
- Limitación de la finalidad
- Minimización de datos
- Exactitud
- Limitación del plazo de conservación
- Integridad y confidencialidad

Privacidad desde el diseño

- Art. 25 RGPD

- Objetivo: pensar en términos de protección de datos desde el mismo momento en que se diseña un tratamiento, un producto o servicio que implica el tratamiento de datos personales, adoptando

  – medidas organizativas y técnicas para integrar en los tratamientos garantías que permitan aplicar de forma efectiva los principios del RGPD.

  – medidas que garanticen que solo se traten los datos necesarios en lo relativo a la cantidad de datos tratados, la extensión del tratamiento, los periodos de conservación y la accesibilidad a los datos.

Incremento categorías especiales de datos

Art. 7 LOPD
Datos especialmente protegidos

- Ideología
- Religión
- Creencias
- Afiliación sindical
- Origen racial
- Salud
- Vida sexual

Art. 9 RGPD
Categorías especiales de datos

- Origen étnico o racial
- Opiniones políticas
- Convicciones religiosas o filosóficas
- Afiliación sindical
- Datos genéticos
- Datos biométricos
- Salud
- Vida sexual
- Orientación sexual

Adiós, inscripción de ficheros en la AEPD

- Obligación derivada de la Directiva 95/46 del Parlamento Europeo y del Consejo, trasladada a la LOPD y RDLOPD.

- **RGPD no contempla esa obligación, la elimina.**
  - **¿Por qué?** Considerando 89:

    Pese a implicar cargas administrativas y financieras, dicha obligación, sin embargo, no contribuyó en todos los casos a mejorar la protección de los datos personales. Por tanto, estas obligaciones generales de notificación indiscriminada deben eliminarse y sustituirse por procedimientos y mecanismos eficaces que se centren, en su lugar, en los tipos de operaciones de tratamiento que, por su naturaleza, alcance, contexto y fines, entrañen probablemente un alto riesgo para los derechos y libertades de las personas físicas

Hola, Registro de las actividades de tratamiento

- ¿Dónde se regula? Art. 30 RGPD

Cada responsable y, en su caso, su representante llevarán un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Dicho registro deberá contener toda la información indicada a continuación:

a) el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos;

b) los fines del tratamiento;

c) una descripción de las categorías de interesados y de las categorías de datos personales;

d)las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;

e)en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;

f) cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;

g) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32, apartado 1.

Hola, Registro de las actividades de tratamiento

Registro de actividades desde la inscripción de ficheros

Servicio de solicitud de copia de la inscripción de ficheros

Para facilitar el registro de actividades que será obligatorio a partir del 25 de mayo, la Agencia ofrece una opción en su Sede electrónica que permite a los responsables descargar el contenido completo de la inscripción de sus ficheros.

No debe notificarse a la AEPD, sólo tenerse a su disposición.

Sector público: debe publicar inventario actividades, accesible por medios electrónicos.

Hola, Registro de las actividades de tratamiento

Ejemplo (guía sectorial AEPD para Ayuntamientos)

· REGISTRO DE ACTIVIDADES SEGURIDAD

ADMINISTRACIÓN LOCAL
Nombre y datos de contacto del responsable (o representante).

ACTIVIDAD DE TRATAMIENTO
Seguridad

LEGITIMACIÓN DEL TRATAMIENTO
Artículo 6.1.e) del RGPD: Cumplimiento de una misión de interés público.

FINES DEL TRATAMIENTO
Garantizar la seguridad de personas e instalaciones

NOMBRE Y DATOS DE CONTACTO DEL DELEGADO DE PROTECCIÓN DE DATOS
Correo electrónico de contacto
Dpd@ayuntamiento.es

CATEGORÍAS DE DATOS PERSONALES.
Respecto al control de acceso: nombre, apellidos, DNI/NIF, empresa/administración.
Respecto a la videovigilancia: Imagen.

CATEGORÍAS DE AFECTADOS.
Ciudadanos que realizan trámites en el Ayuntamiento.
Personas físicas que acuden a reuniones convocadas por el Ayuntamiento.
Personal al servicio del Ayuntamiento.

DESCRIPCIÓN DE LAS MEDIDAS TÉCNICAS Y ORGANIZATIVAS DE SEGURIDAD.
Las medidas de seguridad implantadas corresponden a las aplicadas de acuerdo al Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica y que se encuentran descritas en los documentos que conforman la Política de Seguridad de la Información del Ayuntamiento.

CATEGORÍAS DE DESTINATARIOS DE COMUNICACIONES, INCLUIDOS TERCEROS PAÍSES U ORGANIZACIONES INTERNACIONALES.
Fuerzas y Cuerpos de Seguridad. Juzgados y Tribunales.

TRANSFERENCIAS INTERNACIONALES. DOCUMENTACIÓN DE GARANTÍAS ADECUADAS EN CASO DEL 49.1.
No existen.

Hola, Registro de las actividades de tratamiento

¿Debe obligatoriamente llevar un despacho de abogados este registro?

Art. 30.5 RGPD:

… no se aplicará a ninguna empresa ni organización que emplee a menos de 250 personas, **salvo:**

- que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades.
- o que el tratamiento no sea ocasional.
- o que incluya categorías especiales de datos art. 9 o datos relativos a infracciones/condenas penales

Conclusión: sí deberá llevarlo.

Información al interesado

STC 292/2000, de 30 de noviembre

En fin, son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y, el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que rectifique o los cancele".

Información al interesado

Hasta 24/5/2018

Art. 5.1 LOPD.

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.

Art. 5.2 LOPD

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.

Información al interesado

Hasta 24/5/2018

- Art. 7.1 LOPD.

  De acuerdo con lo establecido en el apartado 2 del art. 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias.

  Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo.

Información al interesado

A partir del 25/5/2018

Se amplía la información a facilitar al interesado

Información al interesado

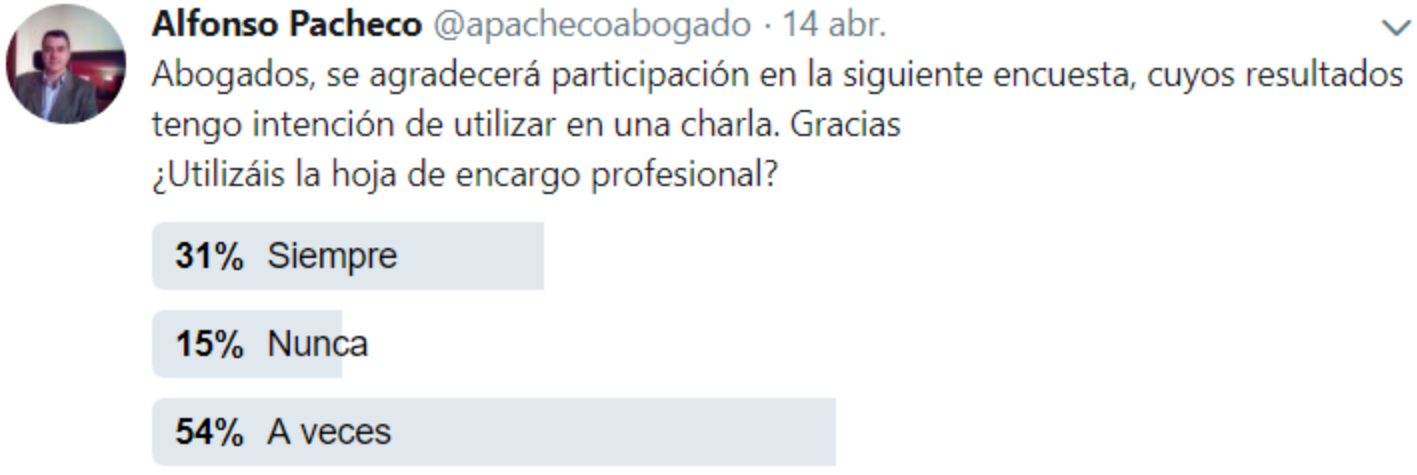
¿ De qué más se debe informar? Art. 13 RGPD

- Datos de contacto del DPD.
- Base jurídica o legitimación tratamiento (art. 6 RGPD).
  - Si esa base es el consentimiento de la posibilidad de retirarlo.
- Plazo o criterios conservación de la información.
- Existencia decisiones automatizadas /elaboración perfiles.
- Previsión transferencias a terceros países.
- Derecho a presentar reclamación ante las Autoridades de Control.
  - https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/modeloclausulainformativa.pdf

¿Cómo ofrecer la información al cliente?

Artículo 12 RGPD:

- De forma concisa (¿con todo lo que hay que decir?), transparente, inteligible y de fácil acceso, con lenguaje claro y sencillo.
- Atención si el destinatario es un niño.
- La información deberá facilitarse por escrito o por otros medios, inclusive, electrónico. **OJO: la carga de la prueba es nuestra**.
- Abogados: hoja de encargo profesional / contrato de servicios
  - ¿Realmente usamos la hoja de encargo?



- Acostumbrarse a dar copia información al cliente ¿Por qué?
- Posibilidad de ofrecer la información en dos capas.

Legitimación y consentimiento

Hasta 24/5/2018.

- **Regla general**, art. 6.1 LOPD: no pueden recabarse/tratarse datos sin consentimiento previo e inequívoco del interesado, salvo que una norma con rango de Ley nos autorice a ello.

- **Excepciones** art. 6.2 LOPD **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 negocial, 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

Legitimación y consentimiento

- Art. 7 LOPD:

  1. De acuerdo con lo establecido en el apartado 2 del art. 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias.

  Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo.

  2. Sólo con el consentimiento **expreso y por escrito** del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias

  3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta **expresamente.**

  Ver informe AEPD 2008-0453:

  https://www.agpd.es/portalweb/canaldocumentacion/informes_juridicos/conceptos/common/pdfs/2008-0453_Consentimiento-al-tratamiento-de-datos-especialmente-protegidos-incorporados-a-fichero.pdf

Legitimación y consentimiento

- ¿Implicaciones prácticas?
  - Ejemplo: accidente de circulación.
    - Contrato a un abogado para que reclame los daños materiales sufridos por mi coche. **No necesito pedir consentimiento**.
    - Contrato a un abogado para que reclame los daños materiales sufridos por mi coche y mis lesiones. **Necesito consentimiento expreso.**
    - Contrato a un abogado para que reclame los daños materiales sufridos por mi coche, mis lesiones y que impida que me hagan una trasfusión, por que soy testigo de Jehová. **Necesito consentimiento expreso y escrito.**

Legitimación y consentimiento

A partir 25/5/2018

Art. 6 RGPD recoge las distintas causas legitimadoras del tratamiento de datos

1.El tratamiento **solo será lícito si se cumple al menos una de las siguientes condiciones**:

a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;

b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;

c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;

d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;

e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;

f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

Consentimiento y legitimación

Artículo 9 RGPD Tratamiento de categorías especiales de datos personales

1.Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física.

2.El apartado 1 **no será de aplicación** cuando concurra una de las circunstancias siguientes:

F) EL TRATAMIENTO ES NECESARIO PARA LA FORMULACIÓN, EL EJERCICIO O LA DEFENSA DE RECLAMACIONES O CUANDO LOS TRIBUNALES ACTÚEN EN EJERCICIO DE SU FUNCIÓN JUDICIAL.

Legitimación y consentimiento

¿Reclamaciones?

Considerando (52) RGPD

Asimismo deben autorizarse excepciones a la prohibición de tratar categorías especiales de datos personales cuando lo establezca el Derecho de la Unión o de los Estados miembros y siempre que se den las garantías apropiadas, a fin de proteger datos personales y otros derechos fundamentales, cuando sea en interés público, en particular el tratamiento de datos personales en el ámbito de la legislación laboral, la legislación sobre protección social, incluidas las pensiones y con fines de seguridad, supervisión y alerta sanitaria, la prevención o control de enfermedades transmisibles y otras amenazas graves para la salud. Tal excepción es posible para fines en el ámbito de la salud, incluidas la sanidad pública y la gestión de los servicios de asistencia sanitaria, especialmente con el fin de garantizar la calidad y la rentabilidad de los procedimientos utilizados para resolver las reclamaciones de prestaciones y de servicios en el régimen del seguro de enfermedad, o con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos. Debe autorizarse asimismo a título excepcional el tratamiento de dichos datos personales cuando sea necesario para la formulación, el ejercicio o la defensa de reclamaciones, ya sea por un procedimiento judicial o un procedimiento administrativo o extrajudicial.

Legitimación y consentimiento

- Posibilidad ya prevista en la Directiva 95/46/CE (ahora derogada por el RGPD, si bien con fecha de efecto 25 de mayo de 2018), pero no contemplada en la LOPD al trasponer la norma europea.

- Art. 8.1:los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad.

- Art. 8.2: Lo dispuesto en el apartado 1 no se aplicará cuando
  - e) el tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos O SEA NECESARIO PARA EL RECONOCIMIENTO, EJERCICIO O DEFENSA DE UN DERECHO EN UN PROCEDIMIENTO JUDICIAL.

Legitimación y consentimiento

Si tenemos que pedirlo ¿Qué entendemos por consentimiento?

RGPD: Artículo 4.11

toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta**,** **ya sea mediante una declaración o una clara acción afirmativa**, el tratamiento de datos personales que le conciernen;

Ese carácter afirmativo elimina la posibilidad de consentimientos por omisión:

"si usted no manifiesta su negativa marcando la casilla dispuesta al efecto entenderemos que autoriza a que le remitamos…."

¿Tratamiento datos personales de la contraparte?

Ver al respecto informe AEPD 2000 (no tiene numeración, del que se adjunta enlace:

https://www.agpd.es/portalweb/canaldocumentacion/informes_juridicos/consentimiento/common/pdfs/2000-0000_Tratamiento-por-abogados-y-procuradores-de-los-datos-de-las-partes-en-un-proceso.pdf

Si lo pido, ¿cómo lo pido? HOJA DE ENCARGO

Delegado de Protección de Datos (DPD)

- Nueva figura introducida por RGPD, artículos 37 a 39.

- Especialista en protección de datos que deben tener **determinadas organizaciones. ¿Cuáles?**

  – Según art 37 RGPD, sin perjuicio de adopción voluntaria por otras, será obligatorio cuando:

  – A) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;

  – b) las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o

  – c) las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10.

Delegado de Protección de Datos (DPD)

- Art. 37.2 RGPD permite a los Estados miembro de la UE fijar su obligatoriedad para determinadas actividades u organizaciones:

  Art. 34 LOPD 2.0 (ojo, en proyecto).

  - Colegios profesionales
  - Centros docentes, Universidades
  - Determinados prestadores servicios de la sociedad de la información (ej: comercio online)
  - Centros sanitarios que mantengan historias clínicas
  - Entidades que se dediquen a emitir informes comerciales acerca de personas o empresas
  - Empresas de seguridad privada
  - Entidades aseguradoras
  - Entidades financieras
  - Empresas de publicidad y prospección comercial (perfiles, preferencias….)
  - Otras…

Delegado de Protección de Datos (DPD)

- ¿Debe obligatoriamente designar un despacho de abogados un DPD?
  - En mi opinión:
    - No encuadrable supuestos art. 37.1 RGPD
    - No encuadrable listado LOPD 2.0
  - Respuesta: NO

Delegado de Protección de Datos

Funciones:

1. El delegado de protección de datos tendrá como mínimo las siguientes funciones:

a) 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 presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;

b) supervisar el cumplimiento de lo dispuesto en el presente 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, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;

c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35;

d) cooperar con la autoridad de control;

e) 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, y realizar consultas, en su caso, sobre cualquier otro asunto.

2. 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.

Delegado de Protección de Datos

5. El delegado de protección de datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39.

6. El delegado de protección de datos podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios.

7. El responsable o el encargado del tratamiento publicarán los datos de contacto del delegado de protección de datos y los comunicarán a la autoridad de control.

1. El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales.

2. El responsable y el encargado del tratamiento respaldarán al delegado de protección de datos en el desempeño de las funciones mencionadas en el artículo 39, facilitando los recursos necesarios para el desempeño de dichas funciones y el acceso a los datos personales y a las operaciones de tratamiento, y para el mantenimiento de sus conocimientos especializados.

3. El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones. No será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones. El delegado de protección de datos rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado.

4. Los interesados podrán ponerse en contacto con el delegado de protección de datos por lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos al amparo del presente Reglamento.

5. El delegado de protección de datos estará obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones, de conformidad con el Derecho de la Unión o de los Estados miembros.

6. El delegado de protección de datos podrá desempeñar otras funciones y cometidos. El responsable o encargado del tratamiento garantizará que dichas funciones y cometidos no den lugar a conflicto de intereses.

Confidencialidad

- De acuerdo con lo dispuesto en el **artículo 10 de la LOPD**, el responsable del fichero y quienes intervengan en cualquier fase de tratamiento de los datos de carácter personal están obligados al **secreto profesional respecto de los mismos y al deber de guardarlos**, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

- De acuerdo con el **artículo 5.f) RGPD** los datos personales serán tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y **confidencialidad**»).

- A su vez, el artículo **32.1.b) RGPD** dice:

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

  – la capacidad de garantizar la **confidencialidad**, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

Confidencialidad

- **Artículo 42 del Estatuto General de la Abogacía** (Real Decreto 658/2001, de 22 de junio):

- 1. Son obligaciones del abogado para con la parte por él defendida, además de las que se deriven de sus relaciones contractuales, el cumplimiento de la misión de defensa que le sea encomendada con el máximo celo y diligencia **y guardando el secreto profesional.**

- **Artículo 5 Código Deontológico Abogacía Española:**
  1.La confianza y confidencialidad en las relaciones entre cliente y abogado, ínsita en el derecho de aquél a su intimidad y a no declarar en su contra, así como en derechos fundamentales de terceros**, impone al abogado el deber y le confiere el derecho de guardar secreto respecto de todos los hechos o noticias que conozca por razón de cualquiera de las modalidades de su actuación profesional,** sin que pueda ser obligado a declarar sobre los mismos como reconoce el artículo 437.2 de la vigente Ley Orgánica del Poder Judicial.

- 2. El deber y derecho al secreto profesional del abogado **comprende las confidencias y propuestas del cliente, las del adversario, las de los compañeros y todos los hechos y documentos de que haya tenido noticia o haya recibido por razón de cualquiera de las modalidades de su actuación profesional.**

- 3. El abogado no podrá aportar a los tribunales, ni facilitarle a su cliente las cartas, comunicaciones o notas que reciba del abogado de la otra parte, salvo expresa autorización del mismo.

- 4. Las conversaciones mantenidas con los clientes, los contrarios o sus abogados, de presencia o por cualquier medio telefónico o telemático, no podrán ser grabadas sin previa advertencia y conformidad de todos los intervinientes y en todo caso quedarán amparadas por el secreto profesional.

Confidencialidad

- 5. En caso de ejercicio de la abogacía en forma colectiva, el deber de secreto se extenderá frente a los demás componentes del colectivo.

- 6. **En todo caso, el abogado deberá hacer respetar el secreto profesional a su personal y a cualquier otra persona que colabore con él en su actividad profesional.**

- 7. **Estos deberes de secreto profesional permanecen incluso después de haber cesado en la prestación de los servicios al cliente, sin que estén limitados en el tiempo.**

- 8. El secreto profesional es un derecho y deber primordial de la Abogacía. En los casos excepcionales de suma gravedad en los que, la obligada preservación del secreto profesional, pudiera causar perjuicios irreparables o flagrantes injusticias, el Decano del Colegio aconsejará al Abogado con la finalidad exclusiva de orientar y, si fuera posible, determinar medios o procedimientos alternativos de solución del problema planteado ponderando los bienes jurídicos en conflicto. Ello no afecta a la libertad del cliente, no sujeto al secreto profesional, pero cuyo consentimiento por sí solo no excusa al Abogado de la preservación del mismo

- Artículo 542 Ley Orgánica del Poder Judicial:

  3. Los abogados deberán guardar secreto de todos los hechos o noticias de que conozcan por razón de cualquiera de las modalidades de su actuación profesional, no pudiendo ser obligados a declarar sobre los mismos

- A tenor de lo anterior, todo el personal/colaborador del responsable está obligado a cumplir con el deber de secreto en relación con los datos personales de los que tenga conocimiento en el desempeño de sus obligaciones.

- Para garantizar el cumplimiento de esta obligación el responsable obtendrá de cada uno de sus empleados y colaboradores, de forma inexcusable, **compromiso escrito de confidencialidad**.

Confidencialidad

Artículo 90

Obligaciones de secreto

1. Los Estados miembros podrán adoptar normas específicas para fijar los poderes de las autoridades de control establecidos en el artículo 58, apartado 1, letras e) y f), en relación con los responsables o encargados sujetos, con arreglo al Derecho de la Unión o de los Estados miembros o a las normas establecidas por los organismos nacionales competentes, a una obligación de secreto profesional o a otras obligaciones de secreto equivalentes, cuando sea necesario y proporcionado para conciliar el derecho a la protección de los datos personales con la obligación de secreto. Esas normas solo se aplicarán a los datos personales que el responsable o el encargado del tratamiento hayan recibido como resultado o con ocasión de una actividad cubierta por la citada obligación de secreto.

2. Cada Estado miembro notificará a la Comisión las normas adoptadas de conformidad con el apartado 1 a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier modificación posterior de las mismas.

Derechos del interesado

- La normativa actual contempla los llamados “Derechos ARCO”

- **A**= **acceso**. Derecho a solicitar y obtener gratuitamente del responsable del fichero información de sus datos de carácter personal sometidos a tratamiento, el origen de esos datos, así como las cesiones que se prevean de los mismos.
- **R**= **rectificación**. Derecho a que se modifiquen los datos que resulten inexactos o incompletos
- **C**= **cancelación**. Derecho a solicitar la supresión de los datos que resulten ser inadecuados o excesivos, si perjuicio del deber de bloqueo. **RGPD SUPRESIÓN**
- **O**= **oposición** Derecho a que no se lleve a cabo el tratamiento o se cese en los supuestos previstos en el art. 34 RDLOPD.

Derechos del interesado

- RGPD añade nuevos derechos:

Limitación del tratamiento

El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:

- a) el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de estos.
- b) el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso.
- c) el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones.
- d) el interesado se haya opuesto al tratamiento, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado

Derechos del interesado

- RGPD añade nuevos derechos:

Portabilidad

Cuando el tratamiento de los datos esté basado en el consentimiento o en un contrato y, además, el tratamiento se realiza por medios automatizados, el interesado tiene derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento.

Derechos del interesado

- RGPD añade nuevos derechos:

Decisiones automatizadas

1.Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

2.El apartado 1 no se aplicará si la decisión:

a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;

b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o

c) se basa en el consentimiento explícito del interesado.

http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/infografias/RGPD_Derechos_ciudadanos_AEPD.pdf

Derechos del interesado

- RGPD añade nuevos derechos:

Decisiones automatizadas

1.Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

2.El apartado 1 no se aplicará si la decisión:

a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;

b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o

c) se basa en el consentimiento explícito del interesado.

http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/infografias/RGPD_Derechos_ciudadanos_AEPD.pdf

¿Nuevo acrónimo? Complicado…

Alfonso Pacheco @apachecoabogado · 14 abr.

#RGPD Adiós al acrónimo ARCO para referirse a los derechos de los interesados. ¿Cuál será el nuevo a la vista de las nuevos derechos incorporados? Tras una sesuda y extensa búsqueda estos son los tres que más me gustan

Derechos del interesado

Principales cambios

- El plazo de atención general pasa de 10 días a un mes, prorrogable 2 meses en caso necesario (complejidad, número de solicitudes)
- Si se presenta solicitud por medios electrónicos sin señalar vía respuesta es válida contestación electrónica.

Derechos del interesado

Al contestar negando la petición formulada no solo debe informarse posible reclamación ante autoridad de control, sino también de posible ejercicio acciones judiciales.

Si petición es manifiestamente infundada, excesiva o repetitiva se puede

- cobrar canon razonable (coste administrativo)
- negarse a actuar

No establece criterio repetición. LOPD 2.0 sugiere seis meses

Carga prueba carácter abusivo responsable

Derechos del interesado

IMPORTANTE: Siempre dejar rastro de la respuesta, de forma que:

- podamos acreditar **contenido**
- podamos acreditar fecha **envío**
- podamos acreditar fecha **recepción/rechazo**

Relaciones Responsable-Encargado tratamiento

- Art. 28 RGPD
- Encargado tratamiento: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos persona-les por cuenta del responsable del tratamiento.

- Deber de diligencia en la selección del encargado tratamiento: *…elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiados, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado.*

Relaciones Responsable-Encargado tratamiento

- Deber de diligencia ya presente en el RDLOPD, art. 20.2:

Cuando el responsable del tratamiento contrate la prestación de un servicio que comporte un tratamiento de datos personales sometido a lo dispuesto en este capítulo deberá velar por que el encargado del tratamiento reúna las garantías para el cumplimiento de lo dispuesto en este Reglamento

Relaciones Responsable-Encargado tratamiento

- Dicha obligación se ha interpretado por la AEPD, en su informe jurídico 0457/2008 en los siguientes términos:

- *El artículo 20. 2 que cita el consultante introduce un poder de supervisión sobre el encargado que se traduce en que el responsable del fichero o tratamiento estará legitimado para realizar controles durante el período de vigencia del contrato para verificar el cumplimiento de las medidas de seguridad establecidas y adoptar las medidas correctoras oportunas.*

Relaciones Responsable-Encargado tratamiento

- ¿Cómo sabemos que el encargado ofrece las garantías suficientes?

  – Primero, el RT debe determinar qué garantías quiere que cumpla-

  – Vías acreditación
    - Adhesión a código de conducta
    - Mecanismo de certificación en protección de datos
    - Aceptación cláusulas tipo aprobadas por Comisión / ente control

  – ¿Y si no se da ninguna de esas circunstancias?

Relaciones Responsable-Encargado tratamiento

De la guía de directrices para la elaboración de contratos entre RT y EN (AEPD, APDCAT, AVPD):

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

Relaciones Responsable-Encargado tratamiento

- ¿De verdad?

- De la herramienta *Facilita* de la AEPD
  - ¿Qué dice en concreto sobre medidas de seguridad?
  - *El encargado del tratamiento y todo su personal se obliga a*

    - *Implantar las medidas de seguridad técnicas y organizativas necesarias para garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.*

¿Dónde está la lista exhaustiva de medidas de seguridad?

Medidas de Seguridad

Hasta 24/5/2018

- LOPD: obliga a los responsables de los ficheros , en nuestro caso al abogado, a implantar ciertas medidas de seguridad respecto de los ficheros que contengan datos personales, reguladas en los artículos 79 a 114 RDLOPD-

- Régimen absolutamente regulado.

- 3 niveles de medidas de seguridad ACUMULATIVOS, en función de la tipología de datos tratados:

  - Básico
  - Medio
  - Alto

Medidas seguridad en el RGPD

A partir 25/5/2018

Art. 32: Tú sabrás lo que haces, que ya eres mayorcito.

En el RGPD, los responsables y encargados establecerán las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado en función de los riesgos detectados en el análisis previo.

Las medidas técnicas y organizativas deberán establecerse teniendo en cuenta:

- El coste de la técnica
- Los costes de aplicación
- La naturaleza, el alcance, el contexto y los fines del tratamiento
- Los riesgos para los derechos y libertades

Medidas seguridad en el RGPD

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

a) la seudonimización y el cifrado de datos personales;

b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

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

Medidas seguridad en el RGPD

- **Búsqueda de estándares:**
  - **¿RDLOPD?**

    El esquema de medidas de seguridad previsto en el Reglamento de Desarrollo de la LOPD no seguirá siendo válido de forma automática tras la fecha de aplicación del RGPD.

    En algunos casos los responsables podrán seguir aplicando las mismas medidas que establece el Reglamento de la LOPD si los resultados del análisis de riesgos previo concluye que las medidas son realmente las más adecuadas para ofrecer un nivel de seguridad adecuado.

    En ocasiones será necesario completarlas con medidas adicionales o prescindir de alguna de las medidas. (Guía conjunta sobre el RGPD de la AEPD, APDCAT, AVPD)

  - **Certificaciones** (ISO)… a pagar (AENOR INTERNACIONAL, S.A.U.)
  - **Códigos de conducta**…. ¿CGAE?
  - **Esquema Nacional de Seguridad AAPP**

Evaluación de impacto

Art. 35 RGPD

Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.

El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.

Evaluación de impacto

Obligatoria en caso de:

a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;

b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o

c) observación sistemática a gran escala de una zona de acceso público.

Evaluación de impacto

Las autoridades de control pueden establecer (y publicar)

- Listado de operaciones de tratamiento para las que **sí** deba llevarse a cabo una evaluación de impacto

- Listado de operaciones de tratamiento para las que **no** deba llevarse a cabo una evaluación de impacto

Evaluación de impacto

Contenido mínimo

a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;
b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;
c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y
d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

Posible consulta a la AEPD si riesgo residual sigue siendo alto

Notificación violaciones seguridad

Artículo 34 RGPD

¿Cuáles hay que notificar? Las que constituyan un riesgo probable para los derechos y libertades de las personas físicas.

¿A quién?

A la autoridad de control competente.

A los propios interesados cuando entrañe un alto riesgo para los derechos y libertades de las personas físicas (salvo art. 34.3 RGPD)

Plazo

Autoridad control: 72 horas

Interesados: sin dilación.

Notificación violaciones seguridad

Contenido de la notificación:

– Naturaleza de la violación (detallada)
– Identificación del DPD
– Posibles consecuencias de la violación para los datos personales
– Medidas adoptadas para solventar la violación y mitigar los efectos

Obligación de documentar la violación: protocolo de incidencias.

La protección de datos como oportunidad de negocio

Formación

Para asesorar en materia de protección de datos es imprescindible formación específica en la materia.

1 cliente = 1 traje a medida

Cada cliente es un mundo distinto, aunque realice la misma actividad que otro al que hemos asesorado.

-ej: escaneado pasaporte

No es lo mismo un cliente del sector privado que uno del sector público.

Tenemos que ser capaces de determinar las **distintas normativas** que se aplican a las actividades de cada cliente.

¿Presupuesto directo?

- Lo primero que hay que hacer **no es presupuestar**.

- Lo primero que hay que hacer es **informarse** sobre el cliente para hacerse una idea de a qué nos enfrentamos.
  - Búsquedas que podamos hacer nosotros por nuestra cuenta
    - Ejemplo: registro de ficheros AEPD/Agencias Autonómicas
    - El cliente tiene presencia en internet porque tiene web.
    - Encontramos información sobre el cliente en San Google.
  - Entrevista informal con el cliente.

Recopilación información y documentación

- ¿Qué le tengo que pedir al cliente?
  - Conveniencia de prepararnos una guía de informaciones y documentos que le debemos pedir al cliente:
    - Estructura de la empresa. ¿administradores?
    - Organigrama y datos contacto
    - Responsables
    - Documento de seguridad si lo tiene
    - Cláusulas informativas LOPD que utilice en distintos supuestos
    - Servicios que le prestan terceros para los que se necesite acceso a datos. Contratos.
    - Servicios que le prestan terceros para los que no se necesite acceso datos. Contratos.
    - Servicios que puede el cliente prestar a terceros para los que se necesite acceso a datos. Contratos.
    - Adherido a sellos /sistemas de calidad
    - Videovigilancia ¿seguridad? ¿control empresarial?
    - Inscripción de los ficheros en la AEPD

Recopilación información y documentación

- ¿Qué le tengo que pedir al cliente?
  - Conveniencia de redactar preguntas para departamento informático:
    - Arquitectura informática de la empresa
    - Inventario equipos
    - Sistema identificación y autenticación usuarios
    - Software de gestión / ofimática
    - Alojamiento en servidores de terceros. ¿Dónde están? Ojo USA/Fuera UE
    - Accesos remotos
    - Medidas de protección del sistema informático
    - Incidencias seguridad
    - Protocolo alta/baja/modificación usuarios
    - Copias de respaldo
    - Soportes
    - Webs (alojamiento, gestión, cookies)
    - Servicios técnicos

Recopilación información y documentación

Ejemplo:

Copias de respaldo
¿Se realizan copias de respaldo de la información contenida en los servidores, equipos y aplicaciones?
Qué tipo/s de copia
Frecuencia
Automatizada o manual
Horario
Software para la realización
Soporte/s en el que se realizan
Lugar de custodia y medidas de seguridad
Sistema de supervisión de la correcta realización de cada copia.
¿Está determinado quién es responsable de la ejecución de las copias?
¿Está todo lo anterior documentado, protocolizado y actualizado?
¿Incluye el protocolo el procedimiento para la recuperación de la información?
¿Se realiza como mínimo semestralmente verificación de la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos, y se documenta?
¿Se controla que los usuarios no guarden información en ubicaciones no correctas (por ejemplo, en el disco duro de su unidad o escritorio)?

Recopilación información y documentación

Ejemplo:

Pen drive / discos duros externos
¿Existe una política de empresa en cuanto al uso de memorias pen drive y discos duros externos? ¿Es conocida por los empleados?
¿Los dispositivos son de la empresa?
¿Los dispositivos permiten el cifrado de la información?
¿Quién decide los usuarios que pueden utilizar este tipo de dispositivos?
¿Existe un protocolo de autorización y listado de personas autorizadas?
Ordenadores portátiles
¿Existen en la empresa ordenadores portátiles?
¿Se guarda en los mismos información de la empresa?
¿Se permite desde los mismos el acceso remoto al sistema informático de la empresa?
¿Los usuarios los pueden sacar de la empresa?
Medidas de protección de esos equipos
¿Quién decide los usuarios que pueden utilizar este tipo de dispositivos?
¿Existe un protocolo de autorización y listado de personas autorizadas?
¿Existe una política de empresa en cuanto al uso de los portátiles? ¿Es conocida por los empleados?

Entrevistas

Las entrevistas personales son muy importantes para determinar los ciclos de todos los tratamientos de datos que se hacen en la organización

- Para qué se tratan datos.
- Base de legitimación
- Qué datos se tratan.
- De qué colectivos.
- Cómo se recogen.
- Cómo se tratan y por quién.
- A quién se comunican y para qué.
- Cómo se guardan y cuánto.
- Si hay transferencias internacionales.
- Sacar a la luz modelos documentales que el cliente no nos había dado.
- Qué hay que corregir.

- ¡¡¡FOTOS!!!

¿Documentación para el cliente?

- Registro de actividades
  - Explicación y registro
  - ¿guía?
- Cláusulas informativas con el contenido que ya hemos visto.
  - Explicación y las cláusulas
  - ¿Primera y segunda capa?
  - Previsión en las mismas de petición de consentimiento cuando es necesario.
    - Casilla no premarcada, siempre con leyenda en sentido afirmativo.
- Protocolo para contratación encargados tratamiento
- Contratos de tratamiento por cuenta de terceros
  - Como RESPONSABLE
  - Como ENCARGADO

¿Documentación para el cliente?

- Análisis de riesgos
  - Cumplimiento normativo
  - Protección de la información
    - Integridad
    - Confidencialidad
    - Disponibilidad
- En su caso, evaluación de impacto
  - Probabilidad e impacto
  - Informe con recomendaciones
- Medidas de seguridad a implantar
- Protocolo ejercicio derechos de los interesados
  - Explicación derechos
  - Protocolo de atención
  - Formulario

¿Documentación para el cliente?

- Protocolo de notificación y resolución de incidencias de seguridad
- Protocolo de notificación de brechas de seguridad
  - AEPD
  - Interesados
- Determinación necesidad DPD
  - Obligatorio
  - Voluntario
  - No se designa
  - Nombramiento y estatuto
  - Notificación AEPD/público en general

¿Documentación para el cliente?

- Calendario acciones pendientes

- Formación

- ¿Formato entrega?
  - Preferentemente electrónico.

- Seguimiento
- Asesoramiento

¿Documentación de ayuda?

- AEPD
  - Guía general del RGPD para responsables
  - Guía sobre el deber de informar
  - Guía para contratos de encargados de tratamiento
  - Guía centros escolares
  - Guía para evaluación de riesgos
  - Guía para realización de EIPD
  - …

GRACIAS POR SU ATENCIÓN