ABOGACÍA TRANSFORMADORA

FUIMOS PRESENTE. SOMOS FUTURO.

XII Congreso Nacional de la Abogacía 2019

8-11 MAYO 2019 VALLADOLID

Custodia y tratamiento de los datos personales de nuestros clientes

Alfonso Pacheco - Teresa Pereyra

Abogacía Española
CONSEJO GENERAL

icava
Ilustre Colegio de Abogados de Valladolid

• Convenciones

- **AEPD** = Agencia Española de Protección de Datos.
- **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.
- **LOPDGDD** = Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y **garantías de los derechos digitales**.
- **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.

• Vuelco normativo

- RGPD deroga Directiva 95/46/CE
  - Uniformidad:
    - Directiva necesitaba trasposición. Cada Estado Miembro, a su manera
    - Reglamento aplicación directamente aplicable en cada Estado miembro.
  - En vigor desde 25 de mayo de 2016
  - Aplicable desde 25 de mayo de 2018

- LOPDGDD deroga LOPD *
  - En vigor desde 7 diciembre 2018
  - Desarrollo/complemento de lo que permite el RGPD

    - * y demás disposiciones que contradigan, se opongan o resulten incompatibles con RGPD y a la propia LOPDGDD

¿Debe un abogado cumplir con la normativa PD?

- Art. 2 RGPD: 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.

- Art. 2.1 LOPDGDD: Lo dispuesto en los Títulos I a IX y en los artículos 89 a 94 de la presente ley orgánica se aplica a cualquier 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.

¿Debe un abogado cumplir con la normativa PD?

- El abogado **SÍ** accede a datos de carácter personal en el desarrollo de sus competencias.
  - **Dato personal** = toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona

- El abogado **SÍ** somete a esos datos de carácter personal a tratamiento automatizado o manual.
  - Tratamiento = cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción

DOS NUEVAS IDEAS

- Conducta proactiva (accountability)

- Privacidad desde el diseño

- **Conducta proactiva: HAY QUE DEJAR MIGUITAS DE PAN POR EL CAMINO…**
- 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** → **DOCUMENTAR**

  ¿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

- Vulneración principios = infracción muy grave

Confidencialidad

Art. 5 LOPDGDD

- Sujeción deber general de confidencialidad art. 5.1f) RGPD
- Esa obligación general será **COMPLEMENTARIA** de los **deberes de secreto profesional** de conformidad con su normativa aplicable.
- Incumplimiento confidencialidad = infracción grave

Confidencialidad

Art. 42 Estatuto General de la Abogacía

Art. 5 Código Deontológico de la Abogacía Española

Art. 542 Ley Orgánica del Poder Judicial

Art. 199.2 Código Penal

Privacidad desde el diseño: hay que ponerse las pilas desde minuto cero

- 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.

¿Todos los datos son iguales en el nuevo régimen legal?

- Categorías especiales art. 9 RGPD
  - Son los del art. 7 LOPD y algunos más (azul)
    - Origen étnico o racial
    - Opiniones políticas
    - Convicciones religiosas o **filosóficas**
    - Afiliación sindical
    - **Datos genéticos**
    - **Datos biométricos**
    - Salud
    - Vida sexual
    - **Orientación sexual**

  - **Hay ausencias en relación antiguo régimen:**
    - **infracciones penales/administrativas (7.2 LOPD)**

¿Todos los datos son iguales en el nuevo régimen legal?

- Datos relativos a condenas e infracciones penales
  - Art. 10 RGPD y 10 LOPD
- Datos relativos a infracciones y sanciones administrativas.
  - Art. 86 RGPD y 27 LOPD
- Todos los demás.
- **¿Importancia de esta clasificación?**
  - Bases de legitimación para tratamiento.
  - Tratar datos sin base de legitimación = infracción muy grave

Registro de Actividades

- Art. 30 RGPD (responsables y encargados)

Documentación de las actividades de tratamiento que lleva a cabo una organización, bien como responsable o como encargado 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**.

Registro de Actividades

- ¿Importancia del RA?
  - conocimiento y control de lo que se hace en nuestra organización y cómo se hace. Ayuda a la toma de decisiones.
  - Coincidencia con buena parte del contenido informativo que debe facilitarse a los interesados cuyos datos se tratan.
- La AEPD sugiere como punto de partida los ficheros inscritos en el Registro General de Protección de Datos.

- **Registro de Actividades**

- ¿Actividades tipo despacho de abogado?
  - Gestión de expedientes
    - En curso
    - Finalizados
  - Facturación y contabilidad
  - Presupuestos
  - Atención derechos
  - Gestión brechas seguridad
  - Contacto (web)
  - Marketing
  - RRHH
  - Videovigilancia

- **Registro de Actividades**
- RA = ¿Para qué tratas datos en tu despacho y cómo lo haces?
- Debemos responder las siguientes **preguntas**:
  - ¿Quién es el responsable de esos tratamientos?
  - ¿Hay un corresponsable?
  - ¿Tienes delegado de protección de datos?
  - ¿Para qué tratas los datos? ¿Estás legitimado?
  - ¿De quién tratas los datos?
  - ¿Qué datos tratas?
  - ¿Realizas cesiones a terceros?
  - ¿Tienes encargados del tratamiento? (bola extra)
  - ¿Cómo tratas los datos? (bola extra)
  - ¿Criterios archivo? (bola extra)
  - ¿Haces transferencias internacionales?
  - ¿Cuánto tiempo conservas los datos?
  - ¿Qué medidas técnicas y organizativas de seguridad aplicas?

- **Registro de Actividades**
- Se aconseja confeccionar plantilla para sistematizar la recogida de información que formará parte del registro de actividades.

- ¿Debo publicarlo/registrarlo en algún lado?
  - No, pero debe tenerse a disposición de la autoridad de control si lo pide.

  - AAPP sí deben hacerlo público (art. 31 LOPDGDD)
    - Ejemplo: AEPD
    - https://www.aepd.es/agencia/transparencia/registro-actividades-tratamiento/index.html

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

- ¿Qué información debo ofrecer?
  - Art. 13 RGPD si se recogen directamente del interesado.
  - Art. 14 RGPD si no se recogen directamente.

Omisión del deber de información = infracción muy grave

Ofrecer información incompleta = infracción grave

- **Información al interesado**

- Identidad + datos contacto responsable tratamiento
- Datos de contacto del DPD.
- Fines del tratamiento
- Base jurídica o legitimación tratamiento (art. 6 RGPD).
  - Si esa base es el consentimiento de la posibilidad de retirarlo.
  - Si es el interés legítimo, especificar cuál es.
- Carácter voluntario o obligatorio facilitación de los datos
- Plazo o criterios conservación de la información.
- Existencia decisiones automatizadas /elaboración perfiles.
- Previsión transferencias a terceros países.
- Ejercicio de derechos reconocidos en la normativa
- Derecho a presentar reclamación ante las Autoridades de Control.

• ¿Cómo ofrecer la información?

- Cláusulas informativas específicas, adaptadas a cada supuesto. No valen cláusulas genéricas. **Ver modelo en web www.privacidadlogica.es**
- 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.
- Atención al canal de recogida: internet
- Documento orientación:
  - https://www.aepd.es/media/guias/guia-modelo-clausula-informativa.pdf

¿Debo informar a la contraparte?

- https://www.aepd.es/informes/historicos/2000-9909.pdf

- NO:
  - Colisión entre 2 derechos fundamentales: protección de datos y tutela judicial efectiva.
  - Ningún derecho fundamental es absoluto, pudiendo ceder ante intereses constitucionalmente relevantes, siempre que el recorte que aquél haya de experimentar se revele como necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho.
  - en nuestra opinión debería darse una prevalencia al derecho consagrado por el artículo 24 de la Constitución, garantizando a su vez las medidas que evitarán un mayor perjuicio a los afectados (en este caso, los oponentes de los clientes cuyos datos son objeto de tratamiento).
  - Ello se funda en que la comunicación a los afectados de las informaciones de que los abogados o procuradores puedan disponer, procedentes de sus clientes, podrían perjudicar, como ya se indicó, el adecuado ejercicio por el propio interesado de las facultades vinculadas con su derecho a obtener la tutela efectiva de los Jueces y Tribunales (al quedar en conocimiento de la otra parte los datos que pudieran ser aportados a juicio en defensa de su derecho).

Bases legitimación tratamiento

- De acuerdo con el **considerando 40 del RGPD**, ***para que el tratamiento sea lícito***, *los datos personales deben ser tratados con el* ***consentimiento*** *del interesado o sobre alguna* ***otra base*** *legítima 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 refiera el presente Reglamento.*

- Por tanto, **la base legitimadora del tratamiento podrá hallarse en las propias disposiciones del RGPD o fuera de él, en otras normas jurídicas del Derecho de la Unión o de los Estados miembros, sean esas disposiciones reguladoras específicamente de la protección de datos personales, como puede ser la nueva LOPD o no, como puede ser la LSSICE:** artículo 21 LSSICE (Ley 34/2002) para remisión comunicaciones comerciales o publicitarias vía electrónica.

Informe jurídico AEPD 2018-0164

• Bases legitimación tratamiento

- **Art. 6.1 RGPD**

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.

Bases legitimación tratamiento

- De las seis, las más habituales en el despacho serán
  - 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

Bases legitimación tratamiento

- **Art. 9.2 RGPD** recoge las condiciones adicionales a las bases art. 6 para tratamiento de **categorías especiales de datos**.
  - 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.

- **¿Reclamaciones?**

  - Considerando (52) RGPD:
    - 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**

Bases legitimación tratamiento

- Datos relativos a **condenas e infracciones penales** Art. 10 LOPDDGG:

- 3. Fuera de los supuestos señalados en los apartados anteriores, los tratamientos de datos referidos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas solo serán posibles cuando sean llevados a cabo por abogados y procuradores y tengan por objeto recoger la información facilitada por sus clientes para el ejercicio de sus funciones.

Bases legitimación tratamiento

- Datos relativos a **infracciones y sanciones administrativas** Art. 27 LOPDDGG:

- 3. Fuera de los supuestos señalados en los apartados anteriores, los tratamientos de datos referidos a infracciones y sanciones administrativas solo serán posibles cuando sean llevados a cabo por **abogados y procuradores** y tengan por objeto recoger la información facilitada por sus clientes para el ejercicio de sus funciones.

Bases legitimación: 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…."

¿Consentimiento tratamiento datos personales de la contraparte?

Ver al respecto informe AEPD 2000-9909 ya citado al hablar de la información.

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

• Plazos conservación y protocolos destrucción

- Los datos personales serán mantenidos de forma que se permita la identificación de los afectados **no más tiempo del necesario para los fines del tratamiento**. Podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo de interés público, fines de investigación científica e histórica o fines estadísticos, sin perjuicio de la aplicación de las correspondientes medidas técnicas y organizativas apropiadas que impone el RGPD.

- Deben tenerse en cuenta, además, los **plazos de prescripción** de las responsabilidades que pudieran ser exigibles al titular del despacho y aquellos plazos legales de conservación que establezcan las normas aplicables a la actividad del despacho.

• Plazos conservación y protocolos destrucción

- Expedientes finalizados.
  - Art. 1964.2 Código Civil: 5 años, acciones personales sin plazo especial.
  - Ojo, plazo válido desde 7/10/2015 (Ley 42/2015).
  - Antes el plazo era de 15 años, se aplica DT 5ª Ley 42/2015
  - **La pregunta del millón**: ¿cuándo entendemos que el expediente está finalizado en temas de familia?
  - Artículo sobre el tema: http://www.privacidadlogica.es/cuantos-anos-puede-un-abogado-guardar-un-expediente-una-vez-finalizado-5-o-15-no-es-la-respuesta-correcta/

• Plazos conservación y protocolos destrucción

Otros supuestos a tener en cuenta para los que hay que fijar plazos

- Presupuestos
- Contabilidad y facturación
- Empleados
- Expediente de atención de derechos
- Proveedores

• Plazos conservación y protocolos destrucción

Necesario establecer **protocolos de eliminación segura** de la información, tanto en soporte informático/electrónico como manual (papel)

- Actas
- Destructoras/empresas especializadas
- Programas borrado seguro

• Delegado de Protección de Datos (DPD)

- Nueva figura introducida por RGPD, artículos 37 a 39.
  - LOPDDGG artículos 34 a 37

- 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.
  - ¿Qué se considera "gran escala"? Concepto no definido en la norma.
    - Considerando 91 RGPD dice que no es gran escala el tratamiento que realiza un abogado

• 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 LOPDDGG

  - Colegios profesionales
  - Centros docentes, Universidades
  - Determinados prestadores servicios de la sociedad de la información (ej: comercio online)
  - Centros sanitarios que mantengan historias clínicas (salvo ejercicio individual por persona física)
  - Entidades que se dediquen a emitir informes comerciales acerca de personas o empresas
  - Empresas de seguridad privada
  - Entidades aseguradoras y reaseguradoras
  - Entidades financieras
  - Empresas de publicidad y prospección comercial (perfiles, preferencias….)
  - Federaciones deportivas (si tratan datos de menores)
  - Otras

• Delegado de Protección de Datos (DPD)

- "ESPECIALISTA" supone que el DPD debe ser una persona formada en la materia y tiene que poder acreditarlo
  - Experiencia
  - Certificación conforme esquema de certificación de DPD de la AEPD
- Puede ser interno o externo
- Independencia
- ¿Funciones? Art. 39 RGPD (mínimos)
  - Informar y asesorar sobre cumplimiento normativa
  - Supervisar el cumplimiento de esa normativa
  - Asesorar en las evaluaciones de impacto
  - Interlocutor frente a los interesados
  - Interlocución y cooperación AEPD
    - Paso previo a posibles procedimientos AEPD.
- Si se nombra, comunicación a la AEPD, cláusulas informativas y visibilidad web.

• Delegado de Protección de Datos (DPD)

- ¿Debe **obligatoriamente** designar un despacho de abogados un DPD?
  - Mi opinión:
    - No encuadrable supuestos art. 37.1 RGPD
    - No encuadrable listado LOPD 2.0
  - Respuesta: NO, pero se debe documentar cómo se llega a esta conclusión (Conducta proactiva) análisis de necesidad.
- Ojo a modificaciones en la normativa: actualizar análisis de necesidad.

• Relaciones con otros abogados

- Mi compañero de despacho es muy majete, pero no tiene porqué acceder a mis expedientes.

- Distintos supuestos:

  - Relación laboral

  - Colaboración a porcentaje bajo mi dirección: ENCARGADO DE TRATAMIENTO. Documentar relación art. 28 RGPD.
  - ¿Está en mi despacho o trabaja desde el suyo?

  - Codirección jurídica con otro compañero: CORRESPONSABILIDAD
    Art. 26 RGPD

• Relaciones con otros abogados

- Artículo 26 RGPD regula la corresponsabilidad y exige
- Distribuir responsabilidades cumplimiento RGPD, con especial mención ejercicio y atención derechos y suministro información arts. 13 y 14 RGPD.
- Documentar funciones y relaciones de los corresponsables en relación con los interesados.
- Poner a disposición de los interesados los aspectos esenciales de los anteriores puntos
    - ¿Cómo? Hoja de encargo

- Contenido del acuerdo:
    - Constancia de esa corresponsabilidad en el tratamiento.
    - Responsabilidad en cuanto al cumplimiento del RGPD
    - Modo de ejercicio de los derechos del interesado
    - Modo de ofrecimiento de la información prevista en el artículo 13 RGPD al interesado
    - Cómo se va a realizar el tratamiento
    - Dónde se va a custodiar el expediente durante la vida del asunto.
    - Control de las entradas y salidas del expediente.
    - Dónde se va a custodiar el expediente una vez finalizado el mismo y hasta el transcurso de los plazos de prescripción de aplicación

- ¿Modelo? https://wp.me/p2LiTh-UE (Privacidad Lógica)

• Relaciones con otros abogados

- Art. 28 RGPD
- Encargado tratamiento: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales 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 con otros abogados

- Acreditar cumplimiento deber de diligencia elección E.T.
  - Establecimiento protocolo
    - Petición de garantías
    - Recepción respuesta y documentación
    - Evaluación y petición aclaraciones o doc complementaria
    - Decisión: contratar o no contratar
    - Recoger relación por escrito
      https://www.aepd.es/media/guias/guia-directrices-contratos.pdf
  - Ojo: abogado colaborador en nuestro despacho distinto contenido si ese colaborador está fuera del despacho

- **Derechos del interesado**

- Hasta ahora, la normativa contemplaba 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

No debe confundirse PORTABILIDAD con la obligación de tener a disposición del cliente sus documentos, recogida en

El artículo 13.12 del Código Deontológico de la Abogacía Española:

La documentación recibida del cliente estará siempre a disposición del mismo, no pudiendo en

ningún caso el Abogado retenerla, ni siquiera bajo pretexto de tener pendiente cobro de honorarios. No obstante podrá conservar copias de la documentación

El artículo 26.3 del Estatuto General de la Abogacía Española:

La venia, excepto caso de urgencia a justificar, deberá ser solicitada con carácter previo y por escrito, sin que el Letrado requerido pueda denegarla y con la obligación por su parte de devolver la documentación en su poder y facilitar al nuevo Letrado la información necesaria para continuar la defensa.

- 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**

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
- RGPD No establece criterio repetición.
  - Sí LOPDGDD para derecho de acceso: 6 meses art. 13.3, salvo que exista causa legítima.
- Carga prueba carácter abusivo del responsable tratamiento

• Derechos del interesado

IMPORTANTE: Establecer protocolo de actuación y conservación.

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

- podamos acreditar **contenido**
- podamos acreditar fecha **envío**
- podamos acreditar fecha **puesta a disposición**

Impedimento/obstaculización/no atención derechos = infracción muy grave /grave

Debe no olvidarse en este ámbito la **preponderancia del derecho constitucional a la defensa letrada** consagrado por el artículo 24 de la Constitución puesto que la comunicación a los afectados de las informaciones de que los abogados o procuradores puedan disponer, procedentes de sus clientes, podrían perjudicar el adecuado ejercicio por el propio interesado de las facultades vinculadas con su derecho a obtener la tutela efectiva de los Jueces y Tribunales (al quedar en conocimiento de la otra parte los datos que pudieran ser aportados a juicio en defensa de su derecho). Por tanto, deberá denegarse, motivadamente, eso sí, las peticiones que formulen las contrapartes del bufete.

• Medidas de Seguridad: Análisis y tratamiento de riesgos

Hasta 24/5/2018

- LOPD obligaba 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 de Seguridad: Análisis y tratamiento de riesgos

A partir 25/5/2018

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 de Seguridad

- ¿Y cuál es el nivel adecuado de seguridad? La norma no dice nada, salvo que debe tenerse en cuenta
  - seudonimización y cifrado de datos personales.
  - Garantizar confidencialidad, disponibilidad, integridad, resiliencia de los sistemas y servicios de tratamiento.
  - Capacidad restauración de la disponibilidad y acceso a los datos personales en caso de incidente físico o técnico
  - Proceso de revisión periódico de las medidas implantadas

- ¿Entonces…? **“Tú sabrás lo que haces, que ya eres mayorcito”**: Analiza los riesgos que existen en tu organización y decide.

• Análisis de riesgos

2 tipos

- Incumplimiento obligaciones normativas: listado AEPD
- Seguridad de la información: riesgos que afecten a estas tres dimensiones

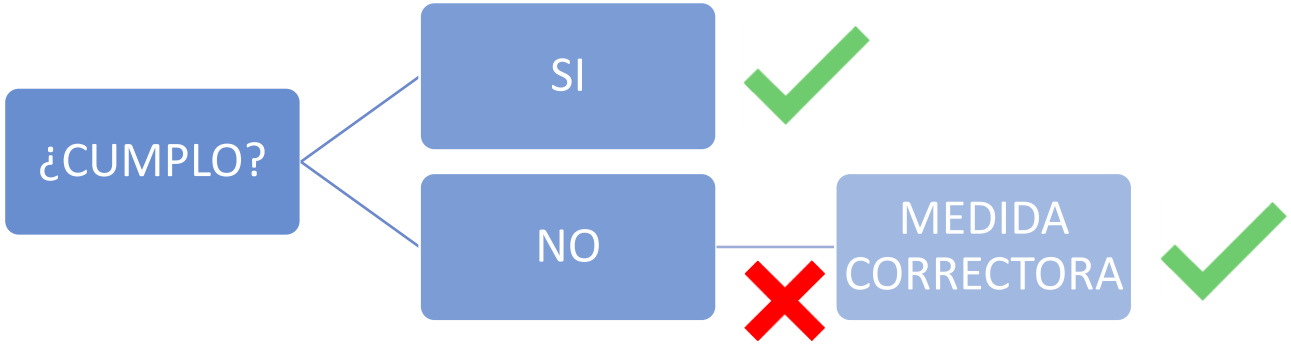
Confidencialidad → acceso ilegítimo a la información

Integridad → modificación de la información

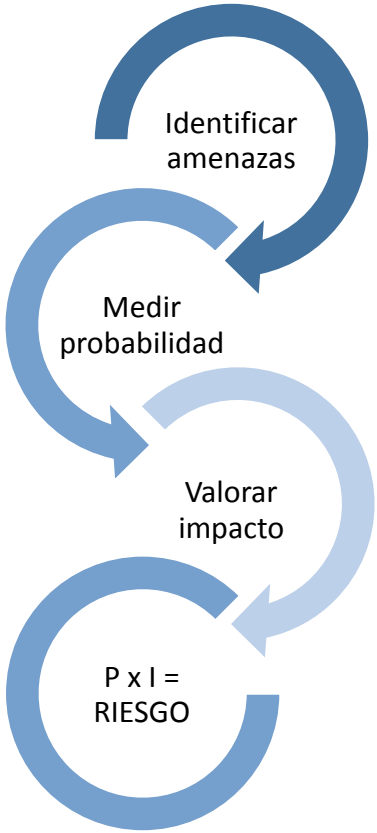
Disponibilidad → no acceso/destrucción

• Análisis de riesgos

- Incumplimiento normativa
  - ¿Se trata la información de acuerdo con todos los principios?
  - ¿Hay base legal para el tratamiento?
  - ¿El consentimiento es válido?
  - ¿Menores?, ¿categorías especiales de datos?, ¿encargados? …



• Análisis de riesgos: Seguridad de la información



- Amenaza = Suceso desfavorable que puede ocurrir y que cuando se materializa provoca un daño en la confidencialidad, disponibilidad e integridad de la información.
- ¿Qué probabilidad hay de que suceda en mi organización?
- ¿Qué impacto tendría sobre los derechos de las personas cuyos datos trato?

PROBABILIDAD **x** IMPACTO **= RIESGO**

• Análisis de riesgos

- ¿Existe un catálogo de amenazas?

  - **Magerit** metodología de análisis y gestión de riesgos de los sistemas de información, libro II, elaborada por el Consejo Superior de Administración Electrónica (https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XFHbHFyuJPY

5.1.2. [N.2] Daños por agua

[N.2] Daños por agua	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: inundaciones: posibilidad de que el agua acabe con recursos del sistema.	

• Tratamiento de riesgos

PROBABILIDAD **x** IMPACTO **= RIESGO**

- Aplico medidas técnico/organizativas para tratar el riesgo
  - Reducción del nivel de riesgo
  - Retención del riesgo
  - Transferencia del riesgo
  - Anulación tratamiento
- Priorizo el tratamiento de riesgos en valores ALTOS.

• Tratamiento de riesgos

- ¿Existen referentes en cuanto a medidas técnico/organizativas?
  - El antiguo RLOPD previo análisis de riesgos y si es suficiente.
  - Anexo A UNE-EN ISO/IEC 27001:2017 Sistemas de Gestión de la Seguridad de la Información.
  - Anexo II 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
- Ojo, siempre que se llegue a la conclusión de que son adecuados tras el oportuno análisis de riesgos.

• Medidas de Seguridad

- ¿Haces copia de seguridad?

  - ¿Cada cuánto?
  - ¿Qué tipo de copia?
  - ¿En qué soporte? ¿Está protegido?
  - ¿Dónde la guardas?
  - ¿Sabes cómo recuperar su contenido?

- ¿Utilizas discos duros externos o memorias usb?
  - ¿Permiten cifrar la información?
  - ¿Los conectas a equipos de terceros?

- ¿Utilizas un ordenador portátil y te lo llevas de paseo?
  - ¿Se puede cifrar el disco?

• Medidas de Seguridad

- ¿Le pasas a ese compañero con el que te llevas tan bien un determinado modelo de demanda que en el fondo es un caso real no anonimizado?

- ¿Recibes a un cliente con 38 expedientes de otros clientes sobre la mesa?

- ¿Cuando te tomas un cafelito al salir del juicio dejas el expediente sobre la mesa del bar?

• Medidas de Seguridad

- ¿Utilizas Whatsapp para comunicarte con el cliente?
  - Aparte de darte la tabarra tooooodoooo el día,
    - ¿Le mandas documentos judiciales?
    - ¿Te manda documentos?

- ¿Usas los ordenadores de las dependencias del colegio abogados en sedes judiciales o biblioteca?
  - ¿Eliminas los documentos que redactas o lo dejas en el escritorio?
  - ¿Cierras tu sesión de drive/onedrive?

• Medidas de Seguridad

Tesoros encontrados en ordenadores sedes colegiales ICAIB en un par de visitas hacia las 13 horas…

- sesiones de Drive
- sesiones de Gmail
- resoluciones judiciales
- escritos redactados por el abogado
- informes policía

ICAIB tiene previsto borrado de todo lo que se ha ido acumulando a lo largo del día

• Medidas de Seguridad

- ¿Guardas todos los expedientes que has llevado en tu vida profesional, que ya va para 30 años?
- ¿Utilizan tus hijos tu ordenador portátil del trabajo?
- ¿Utilizan tus hijos tu teléfono móvil para jugar en la consulta del médico?
- ¿Usas contraseñas seguras en el ordenador?. ¿Las cambias periódicamente?

• Medidas de Seguridad

- ¿Tienes instalado un programa antivirus?. ¿Es de pago?. ¿Lo actualizas?
- ¿Tu teléfono móvil tiene medidas de protección?
- ¿Tus compañeros de despacho acceden alegremente a tus expedientes?

• Medidas de Seguridad

- ¿Tienes destructora de papel?
  - Si la tienes, ¿destruye también CD/DVD?
- ¿Cómo eliminas una cantidad enorme de papel?
- ¿Cómo eliminas los archivos informáticos del ordenador/soportes?
  - ¿papelera de reciclaje y va que chuta?
  - ¿programa de borrado seguro?
- ¿Documentas lo que eliminas?

• Violaciones o brechas de seguridad

RGPD va más allá de lo exigido hasta ahora en materia de incidentes de seguridad.

Determinados incidentes pueden suponer una violación o brecha de seguridad de los datos personales.

todo incidente que ocasionen 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

Si constituye un riesgo probable para los derechos y libertades de las personas físicas HAY QUE NOTIFICARLA A LA AUTORIDAD DE CONTROL COMPETENTE. **72 HORAS**

Si el riesgo no solo es probable, sino **ALTO**, HAY QUE NOTIFICARLA TAMBIÉN A LOS PROPIOS **INTERESADOS** (excepciones en el art. 34. RGPD). SIN DILACIÓN. **DAÑO REPUTACIONAL**

• Violaciones o brechas de 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.

Documentación ayuda: guía AEPD

• Violaciones o brechas de seguridad

DETECCIÓN
- Alerta interna
- Activación protocolo

ANÁLISIS Y EVALUACIÓN
- Recogida información
- Clasificación
- Contención temprana
- Plan de respuesta

RESPUESTA
- Acciones correctivas incidente
- Auditoría
- Controles periódicos

NOTIFICACIÓN
- AEPD – 72h
- INTERESADO – Sin dilación

SEGUIMIENTO Y CIERRE
- Informe final

1. Medidas de Seguridad: Análisis y tratamiento de riesgos

2. Gestión del incidente

GRACIAS