PASO A PASO EN LA ADAPTACIÓN A LA NUEVA NORMATIVA SOBRE PROTECCIÓN DE DATOS DE DESPACHOS PROFESIONALES

ÍNDICE:

- 1. DELIMITACIÓN DEL SECTOR DE ACTIVIDAD
- 2. IDENTIFICACIÓN DE LA TIPOLOGÍA DE DATOS TRATADA. DATOS ESPECIALMENTE PROTEGIDOS. OTROS DATOS ESPECIALMENTE PROTEGIDOS
- 3. CONFECCIÓN DEL REGISTRO DE ACTIVIDADES DE TRATAMIENTO
- 4. ANÁLISIS DE RIESGOS. CICLO DE VIDA DE LOS DATOS, DETERMINACIÓN DE PROBABILIDAD DE MATERIALIZACIÓN Y VALORACIÓN FINAL DEL ANÁLISIS
- 5. REALIZAR UNA EVALUACIÓN DE IMPACTO EN MI DESPACHO PROFESIONAL. IMPACTO ACEPTABLE E IMPACTO ELEVADO
- 6. DEBER DE CONSULTA PREVIA
- 7. ¿NECESITA MI DESPACHO UN DELEGADO DE PROTECCIÓN DE DATOS (DPD)?
- 8. REVISIONES PERIÓDICAS. LISTADO DE CUMPLIMIENTO NORMATIVO
- 9. ACTUALIZACIÓN DE TEXTOS LEGALES, CLÁUSULAS Y DOCUMENTACIÓN TÉCNICA

1. Delimitación del sector de actividad

- **¿Cuáles son los sectores “delicados”?**
  - *Actividades de servicios sociales*
  - *Actividades políticas, sindicales o religiosas*
  - *Actividades bancarias y financieras*
  - *Sanidad*
  - *Seguridad*
  - *Servicios de telecomunicaciones*
  - *Solvencia patrimonial y crédito*
  - *Videovigilancia masiva*

Entonces, ¿el ejercicio de la abogacía no se trata de una actividad “delicada”?

En atención a lo dispuesto en la normativa, no. Sin embargo, por los tipos de datos que se tratan en el ejercicio de esta profesión (véanse, datos de salud, ideología política, creencias, etc.), el siguiente paso consistirá en identificar la tipología concreta de nuestro despacho, pues dependiendo de ella nos veremos en la obligación de realizar un análisis de riesgo exhaustivo que conduzca a una Evaluación de Impacto o un análisis de riesgos de corte básico.

2. IDENTIFICACIÓN DE LA TIPOLOGÍA DE DATOS TRATADA. DATOS ESPECIALMENTE PROTEGIDOS. OTROS DATOS ESPECIALMENTE PROTEGIDOS

¿Qué tipología de datos puedo encontrar en mi despacho profesional?

A) Datos especialmente protegidos

- Afiliación sindical (excepto cuotas sindicales)
- Condenas o infracciones penales
- Datos biométricos distintivos de un individuo
- Datos genéticos
- Geolocalización
- Opiniones políticas o religión
- Origen étnico o racial
- Salud física o mental
- Vida sexual u orientación sexual

B) Otros datos especialmente protegidos

- Análisis de perfiles
- Asociados o miembros de partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas, fundaciones y otras entidades sin ánimo de lucro, con finalidad política, filosófica, religiosa o sindical
- Control sanitario o venta de medicamentos
- Historial clínico o sanitario
- Prestación de servicios de explotación de redes públicas o servicios de comunicación electrónica (proveedores de servicios de Internet)
- Publicidad y prospección comercial masiva a potenciales clientes

C) Datos básicos:

- Nombre y apellidos del cliente
- Domicilio del cliente
- Número de cuenta bancaria
- Imágenes de cámaras de videovigilancia
- Datos académicos o profesionales del cliente
- Número de teléfono
- Dirección de correo electrónico
- Perfiles de redes sociales
- Dirección IP
- Fotografías o imágenes en vídeo del cliente
- Otros datos de carácter identificativo no mencionados hasta aquí

3. CONFECCIÓN DEL REGISTRO DE ACTIVIDADES DE TRATAMIENTO

Una vez que hemos determinado qué tipo de datos va a tratar nuestro despacho (las tres categorías expuestas anteriormente), es tarea del Responsable de los tratamientos la identificación y confección del Registro interno de las actividades de tratamiento que lleve a cabo el despacho (artículo 30 del RGPD).

A mayor abundamiento, es destacable que esta obligación legal también recae sobre los Encargados de tratamiento.

¿Qué información debe contener este Registro?

- Nombre y datos de contacto del responsable (y corresponsable, si lo hubiese)
- Nombre y datos de contacto del representante del responsable
- Nombre y datos de contacto del Delegado de Protección de Datos (si lo hubiese)
- Finalidad del tratamiento
- Descripción de las categorías de interesados y categorías de datos personales tratadas
- Categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales (incluidos los enmarcados en terceros países u organizaciones internacionales)
- Transferencias internacionales de datos (siempre que se lleven a cabo), con los datos identificativos del país u organización internacional a la que se transfieren
- Plazos de conservación y/o supresión de los datos de nuestros clientes
- Descripción general de las medidas técnicas y organizativas de seguridad que nuestro despacho aplique

4. ANÁLISIS DE RIESGOS. CICLO DE VIDA DE LOS DATOS, DETERMINACIÓN DE PROBABILIDAD DE MATERIALIZACIÓN Y VALORACIÓN FINAL DEL ANÁLISIS

Llegados a este punto, hemos delimitado el sector concreto de actividad de nuestro despacho profesional y hemos identificado las categorías de datos personales que tratamos de nuestros clientes. Por tanto, el siguiente paso para continuar con la adaptación normativa consiste en llevar a cabo un análisis de los riesgos que nuestros tratamientos puedan suponer de cara a los derechos y libertades de las personas afectadas; esto es, nuestros **clientes** o **potenciales clientes**.

1º. Confección del ciclo de vida de los datos

En este punto, cada despacho profesional debe documentar el ciclo que siguen los datos personales, desde el momento en el que son recabados, hasta el momento en el que tiene lugar la supresión. A estos efectos, el ciclo de vida de los datos debe responder a las siguientes cuestiones:

a) ¿Cómo se capturan los datos?

b) ¿Cómo se almacenan los datos? (en papel, a nivel informatizado o de forma mixta)

c) ¿Cuál es la clasificación de los datos personales seguida por el despacho?

d) ¿Cuál/cuáles serán los usos o tratamientos de los datos recabados?

e) ¿Cuáles son las partes implicadas en el tratamiento de datos? (equipos informáticos, interesados, personal con acceso a datos y soportes de información)

f) ¿Se producirá alguna cesión o transferencia internacional? En caso afirmativo, ¿a qué entidades se cederán los datos?

g) ¿Cuánto tiempo conservaremos los datos hasta su supresión?

2º. Determinación de riesgos y nivel de probabilidad

En este punto, el Responsable o persona designada por este, debe llevar a cabo un listado completo con los riesgos asociados a la privacidad y protección de datos que puedan afectar a la entidad. Una vez confeccionado el listado, se debe asignar un grado de probabilidad de materialización dichos riesgos.

A estos efectos, ¿qué tipo de riesgos podemos encontrar en nuestro despacho profesional?

a) Ataques intencionados

b) Errores o fallos no intencionados

c) Desastres naturales

d) Desastres industriales

a) ¿Qué tipos de ataques intencionados pueden existir?

- Abuso de privilegios de acceso
- Acceso no autorizado
- Alteración de secuencias
- Ataque u ocupación
- Difusión de software dañino
- Divulgación de información
- Envío incorrecto de mensajes
- Extorsión y/o abuso de la buena fe
- Indisponibilidad del personal
- Interceptación de información (escuchas no autorizadas)
- Manipulación de los registros de actividad (logs) y/o de la configuración
- Manipulación de programas y/o equipos
- Modificación o destrucción deliberada de la información
- Repudio
- Robo
- Suplantación de identidad del usuario
- Uso no previsto

b) ¿Qué tipo de errores o fallos no intencionados pueden existir?

- Alteración accidental de la información
- Caída del sistema por agotamiento de recursos
- Deficiencias en la organización
- Destrucción de información
- Difusión de software dañino
- Errores de los usuarios
- Errores de mantenimiento/actualización de equipos (hardware)
- Errores de monitorización
- Errores de redirección/escapes de información
- Errores del administrador/es
- Indisponibilidad del personal interno
- Pérdida de equipos
- Vulnerabilidades y errores de mantenimiento/actualización de programas (software)

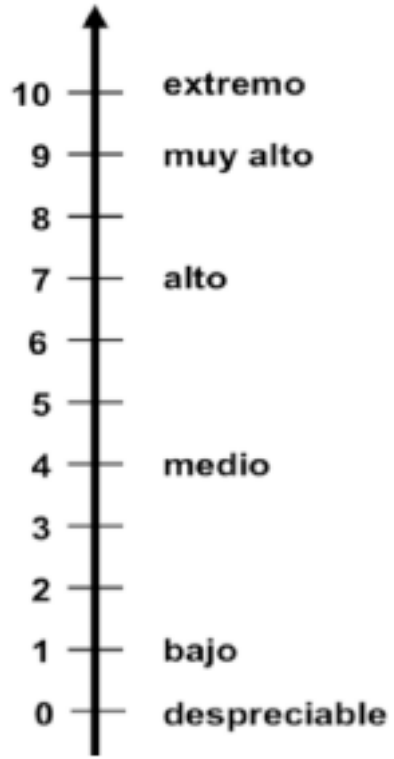
c) Desastres naturales

- Daños por agua
- Fuego, incendio
- Desastres naturales en términos generales

d) Desastres industriales

- Avería técnica
- Captación ilegítima de información mediante emanaciones electromagnéticas
- Condiciones inadecuadas de temperatura o humedad
- Contaminación
- Daños por agua
- Degradación de los soportes de almacenamiento de la información
- Desastres industriales
- Fuego, incendio

Criterio de valoración del nivel de probabilidad



valor		*criterio*
10	extremo	daño extremadamente grave
9	muy alto	daño muy grave
6-8	alto	daño grave
3-5	medio	daño importante
1-2	bajo	daño menor
0	despreciable	irrelevante a efectos prácticos

3º. Valoración final y conclusiones

De acuerdo con el análisis realizado, una vez asignado el nivel de probabilidad de materialización de los riesgos, el responsable del despacho (o la persona designada por él) debe formular la valoración final en conjunto con las correspondientes conclusiones. Este informe final debe motivar la necesidad de implementar las diferentes medidas técnicas y organizativas tendentes a la salvaguarda de los derechos y libertades de los interesados.

Así las cosas, es posible que el Análisis de riesgos arroje dos resultados generales:

a) Bajo riesgo → redacción de informe sobre medidas de salvaguarda a implementar → exención de la obligación de realizar una EIPD

b) Alto riesgo → redacción de informe sobre la necesidad de realizar una EIPD → obligación de realizar una EIPD

5. REALIZAR UNA EVALUACIÓN DE IMPACTO (EIPD) EN MI DESPACHO PROFESIONAL. IMPACTO ACEPTABLE E IMPACTO ELEVADO

De acuerdo con lo dispuesto en el artículo 35 del RGPD, la EIPD sólo será obligatoria en los siguientes supuestos:

- Utilización de nuevas tecnologías en el tratamiento de datos personales
- Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles
- Tratamiento “a gran escala” de categorías especules de datos o de datos relativos a condenas e infracciones penales
- Observación sistemática “a gran escala” de una zona de acceso público
- Que entrañe un **alto riesgo** para los derechos y libertades de las personas físicas

Por tanto…

Si tras la realización del análisis de riesgo comprobamos que nuestro despacho profesional está sometido a un alto nivel de probabilidad de que se materialicen los riesgos identificados, habiéndolo consignado en el informe correspondiente, estaremos ante la obligación de realizar una EIPD en los términos que la normativa exige

¿Qué debe incluir la EIPD de su despacho?

- A) Descripción sistemática de las operaciones de tratamiento previstas en las que se refleje la finalidad del tratamiento y el interés legítimo perseguido por el despacho profesional (como Responsable)
- B) Evaluación de la necesidad y proporcionalidad de las operaciones de tratamiento con respecto a su finalidad
- C) Evaluación de los riesgos para los derechos y libertades de los interesados
- D) Medidas previstas para afrontar los riesgos, tomando en consideración los derechos e intereses legítimos de los interesados y de otras personas afectadas

Resultado de la EIPD

A) Impacto aceptable

Puede llevar a cabo el tratamiento concreto

B) Impacto elevado

Debe abstenerse de llevar a cabo el tratamiento concreto.

En este caso, debe formular una consulta previa a la Agencia Española de Protección de Datos y solicitar su asesoramiento

6. Deber de consulta previa

Como se ha visto, en virtud de lo dispuesto en el artículo 36 del RGPD, **siempre que el resultado de la EIPD arroje un alto riesgo si no se toman las medidas para mitigarlo**, el despacho profesional (en calidad de responsable del tratamiento) debe buscar la aprobación de la AEPD a través de la consulta previa.

¿Qué aspectos deben indicarse en la consulta por parte del despacho profesional?

a) Las responsabilidades del responsable, los corresponsables (si los hubiera) y los encargados de tratamiento

b) La finalidad y los medios del tratamiento previsto

c) Las medidas y garantías a implementar para proteger los derechos y libertades de los interesados

d) Si lo hubiese, los datos de contacto del DPD

e) El contenido documental de la EIPD realizada

f) Cualquier otra información que pueda solicitar la AEPD

7. ¿NECESITA MI DESPACHO UN DELEGADO DE PROTECCIÓN DE DATOS (DPD)?

A falta de una normativa nacional que amplíe el abanico de designaciones obligadas, en virtud de lo dispuesto en el artículo 37.1 del RGPD es posible afirmar que se necesitará un DPD en los siguientes supuestos:

a) Cuando el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los Juzgados y Tribunales (véanse los Colegios de Abogados o Procuradores)

b) Cuando la actividad principal del responsable o encargado requiera una observación habitual y sistemática de interesados a gran escala

c) Cuando la actividad principal del responsable o el encargado consista en el tratamiento "a gran escala" de categorías especiales de datos o datos relativos a condenas o infracciones penales

d) Cuando, de manera potestativa, así lo decida el responsable o encargado de tratamiento

→ Solo si nos encontramos ante uno de los anteriores condicionantes, nuestro despacho profesional necesitará contar con un DPD

8. REVISIONES PERIÓDICAS. LISTADO DE CUMPLIMIENTO NORMATIVO

De acuerdo con el deber de proactividad y de demostración de la diligencia debida que exige el RGPD para los responsables de tratamiento, una vez hayamos confeccionado con éxito la EIPD, podremos afirmar que nuestro despacho se encuentra temporalmente adaptado a la nueva normativa.

¿Por qué *temporalmente* adaptado?

Porque la exigencia de cumplir con la normativa no debe probarse sólo una vez, sino durante toda la vida de los datos y/o tratamientos que realice el despacho.

¿Cómo se puede probar el cumplimiento normativo a lo largo del tiempo?

A través de la realización de auditorías de comprobación o revisiones periódicas, en las que se analicen todos los extremos previamente evaluados. Resulta muy útil para esta labor el cumplimiento de **listados de cumplimiento normativo.**

¿Qué aspectos deben verificarse en el listado de cumplimiento normativo?

- **Criterios generales sobre el RGPD:**
  - *Licitud o bases de legitimación del tratamiento*
  - *Protección de datos desde el diseño y por defecto*
  - *Principios relativos al tratamiento*
- **Derechos de los interesados:**
  - *Decisiones individuales automatizadas, incluida la elaboración de perfiles*
  - *Derecho a la limitación del tratamiento*
  - *Derecho a la portabilidad de los datos*
  - *Derecho de acceso*
  - *Derecho de oposición*
  - *Derecho de rectificación*
  - *Derecho a la supresión (derecho al olvido)*
  - *Información a facilitar cuando los datos no se obtienen del interesado*
  - *Información a facilitar cuando los datos se obtienen del interesado*
  - *Información al interesado ante rectificación, supresión o limitación del tratamiento*
  - *Transparencia en la información*

- Consentimiento:
  - *Condiciones para el consentimiento*
  - *Consentimiento de niños en relación con los servicios de la sociedad de la información*
- Registro de actividades
- Tipología de tratamientos:
  - *Tratamiento de categorías especiales de datos*
  - *Tratamientos relativos a condenas e infracciones penales*
  - *Tratamientos que no requieren identificación*
- Encargado de tratamiento
- Seguridad del tratamiento y notificación de brechas de seguridad

9. ACTUALIZACIÓN DE TEXTOS LEGALES, CLÁUSULAS Y DOCUMENTACIÓN TÉCNICA

Con carácter complementario a lo visto hasta este punto, el paso último para adaptar la actividad de nuestro despacho profesional consiste en la actualización de todos los textos, cláusulas o coletillas legales que incorporemos en nuestros documentos (véanse las hojas de encargo, facturas, correos electrónicos enviados, etc.).

A estos efectos, para nuestro despacho profesional debemos contar con los siguientes textos legales:

- El cartel informativo (preferiblemente, por capas)
- Cláusula legal sobre protección de datos para facturas emitidas
- Cláusula legal sobre protección de datos para correos electrónicos (con y sin publicidad o prospección comercial)
- Cláusula legal sobre protección de datos para los contratos o formularios suscritos (incluida la hoja de encargo)
- Documento informativo sobre las obligaciones de los profesionales pertenecientes al despacho (incluidos los alumnos que realicen prácticas profesionales)

En caso de que el despacho cuente con **página web….**

- *Aviso legal adaptado a la actividad*
- *Política de privacidad y uso de cookies*

Documentación técnica (anteriormente, Documento de Seguridad):

Finalmente, una vez su que despacho haya atravesado con éxito las diferentes fases de adaptación a la nueva normativa, con inclusión de las diferentes revisiones periódicas que el responsable (o DPD, en su caso) fuese realizando, se debe recopilar toda la documentación técnica que se ha ido generando desde el inicio del procedimiento.

¿Por qué recopilar toda la documentación?

Porque al recopilar todos los pasos que nuestro despacho profesional va tomando al objeto de cumplir la normativa, estamos demostrando constantemente la diligencia exigible y el respeto al fundamental principio de proactividad

¿Cuál debe ser el contenido de la documentación técnica?

- *Registro de Actividades de Tratamiento*
- *Informe valorativo sobre análisis de riesgos realizado*
- *Informe valorativo sobre la necesidad o no de realizar EIPD*
- *En su caso, informe completo sobre el proceso de EIPD y sus conclusiones*
- *Listado de cumplimiento normativo actualizado*
- *Listado identificativo del personal que compone el despacho*
- *Listado identificativo del conjunto de activos que dispone el despacho (equipos informáticos, soportes de almacenamiento, etc.)*
- *Medidas de salvaguarda adoptadas por el despacho profesional*
- *En su caso, nombramiento legal de DPD y datos identificativos*
- *Informes de Auditoría (externos o internos)*
- *Informes de revisiones periódicas*