15 de febrero

CEEI ELCHE

# Novedades protección de datos para las Pymes

GENERALITAT VALENCIANA

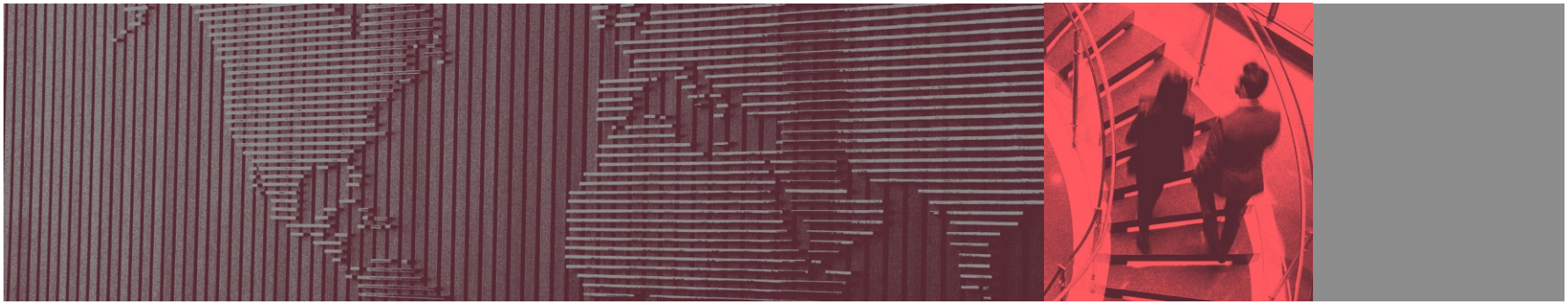
IVACE INSTITUT VALENCIÀ DE COMPETITIVITAT EMPRESARIAL

UNIÓN EUROPEA
Fondo Europeo de Desarrollo Regional

*Una manera de hacer Europa*

"Proyecto cofinanciado por los Fondos FEDER, dentro del Programa Operativo FEDER de la Comunitat Valenciana 2014-2020"

# Objetivo mayo 2018: el nuevo régimen legal del Reglamento General de Protección de Datos.



**Javier Aliño Sehwerert**
Asociado del Área de Litigación y Arbitraje

Elche, 15 de febrero de 2018.


# INTRODUCCIÓN

*"¿Cuándo has dicho que se empieza a aplicar?"*

- Aplicable a partir del 25 de mayo de 2018, tras 2 años de vigencia.
- Nueva LOPD: Proyecto en trámite de enmiendas.
- Aplicabilidad directa del RGPD.
- Mecanismos de revisión cada 4 años, modificable conforme a la evolución de la tecnología.
- Régimen sancionador.

*"Pero, si mi empresa ya cumple con la normativa vigente."*

Tiene notificado e inscritos los ficheros.


Recoge los datos personales en cumplimiento de los principios de calidad, información y consentimiento.

Permite y encauza el ejercicio de los derechos ARCO.


Tiene un documento de seguridad que prevé todas las medidas de la ley.

Vela por la seguridad de los datos comunicados

*"¿Y por qué ahora otra norma en materia de protección de datos?"*

- Antigüedad de la norma vigente: Directiva 1995 y LOPD 1999. No dan cobertura a nuevas realidades: multicanalidad, big data, profiling, digitalización, redes sociales, mensajería instantánea, etc.
- Armonización de la normativa UE: La Directiva 1995 no es directamente aplicable, necesita transposición en cada Estado Miembro.
- Nuevas reglas del Mercado Único: Impulso al comercio electrónico, se busca generar confianza en el consumidor. Complementariedad con otras normas (Directiva e-Privacy, Directiva NIS).
- Cambios en el panorama social: Reconocimiento de nuevos derechos (olvido, portabilidad) y adecuación a la nueva realidad. El ciudadano quiere tener el control de sus datos.

*"Entonces, ¿lo que tengo ahora mismo no vale de nada?"*

Cambio de enfoque: Legalismo vs "Accountability"

- Enfoque de riesgo: Conocimiento de la empresa, de los datos que trata y los tratamientos que realiza.
- Autoevaluación de los riesgos específicos.
- Responsabilidad proactiva de la empresa (prevención).
- Adopción de las medidas más adecuadas.
- El responsable debe poder garantizar y demostrar que cumple con el RGPD.
- Protección desde el diseño: Planificar los tratamientos estableciendo medidas de protección de los datos objeto del tratamiento.
- Protección por defecto: Aplicación de las medidas menos invasivas (alcance del tratamiento, conservación, accesibilidad)

*"¿Saben ustedes dónde está su Documento de Seguridad?"*


Analogía de velocidad

*"Pero, a ver, entonces, ¿exactamente qué es lo que cambia?"*

- **La necesidad de contar con un registro de actividades del tratamiento**, que permite trazar un mapa de los tipos de datos y sus flujos. Sustituye a los antiguos ficheros y Documento de Seguridad. Contenido:

  - Nombre y datos de contacto del responsable, representante y delegado.
  - Fines del tratamiento.
  - Categorías de interesados y de datos personales.
  - Categorías de destinatarios a los que se han comunicado o vayan a comunicarse los datos.
  - Transferencias a internacionales de datos (alojamiento de datos)
  - Plazos previstos para la supresión de las diferentes categorías de datos (límite de conservación de los datos).
  - Descripción general de las medidas de seguridad (acceso, trazabilidad, seguridad física y lógica).

- **No aplicable a empresas de menos de 250 empleados**, salvo que el tratamiento pueda suponer un riesgo para sus derechos y libertades, no tenga carácter ocasional o incluya categorías especiales de datos o datos relativos a condenas y delitos penales.

- **Información al interesado**: Como hasta ahora, se debe proporcionar información concisa, transparente, inteligible y accesible, en un lenguaje **claro y sencillo**. Se ha introducido la posibilidad de proporcionar la información por medio de **iconos estandarizados**. Se debe informar (previa o posteriormente, según el momento de la recogida) sobre:

  - Identidad y datos de contacto del responsable, representante y delegado.
  - Fines y base jurídica del tratamiento.
  - Destinatarios o categorías de destinatarios.
  - Transferencias a terceros países.
  - Plazo de conservación o, si no es posible, criterios para determinar el plazo.
  - Derechos de acceso, rectificación, supresión, oposición, limitación y portabilidad.
  - Derecho a presentar reclamación ante autoridad de control.
  - Si existe obligación legal o contractual de facilitar los datos, o son necesarios para suscribir el contrato; si es obligatorio facilitar los datos y las consecuencias de no facilitarlos.
  - La existencia de decisiones automatizadas y elaboración de perfiles, indicando la lógica aplicada y las consecuencias previstas de dicho tratamiento para el interesado.
  - Si no fueron proporcionados por el interesado, el origen de los datos y las categorías de los datos.

- Sistema de información por capas (¿vía telefónica?).
- Registro de cumplimiento de obligaciones informativas.
- Datos no obtenidos del interesado: antes de un mes o en la primera comunicación.

| Epígrafe | Información básica (1ª capa, resumida) | Información adicional (2ª capa, detallada) |
|---|---|---|
| ***"Responsable"*** (del tratamiento) | Identidad del Responsable del Tratamiento | Datos de contacto del Responsable |
| | | Identidad y datos de contacto del representante |
| | | Datos de contacto del Delegado de Protección de Datos |
| ***"Finalidad"*** (del tratamiento) | Descripción sencilla de los fines del tratamiento, incluso elaboración de perfiles | Descripción ampliada de los fines del tratamiento |
| | | Plazos o criterios de conservación de los datos |
| | | Decisiones automatizadas, perfiles y lógica aplicada |
| ***"Legitimación"*** (del tratamiento) | Base jurídica del tratamiento | Detalle de la base jurídica del tratamiento, en los casos de obligación legal, interés público o interés legítimo. |
| | | Obligación o no de facilitar datos y consecuencias de no hacerlo |
| ***"Destinatarios"*** (de cesiones o transferencias) | Previsión o no de Cesiones | Destinatarios o categorías de destinatarios |
| | Previsión de Transferencias, o no, a terceros países | Decisiones de adecuación, garantías, normas corporativas vinculantes o situaciones específicas aplicables |
| ***"Derechos"*** (de las personas interesadas) | Referencia al ejercicio de derechos. | Cómo ejercer los derechos de acceso, rectificación, supresión y portabilidad de sus datos, y la limitación u oposición a su tratamiento |
| | | Derecho a retirar el consentimiento prestado |
| | | Derecho a reclamar ante la Autoridad de Control |
| ***"Procedencia"*** (de los datos) | Fuente de los datos (cuando no proceden del interesado) | Información detallada del origen de los datos, incluso si proceden de fuentes de acceso público |
| | | Categorías de datos que se traten |

Fuente: Guía AEPD sobre el deber de informar.

- **Tratamiento de los datos**: El RGPD vincula el cumplimiento de una serie de obligaciones a la legalidad de os datos, debiendo cumplirse con los siguientes principios en relación con el tratamiento de los mismos:

  - Principios de transparencia y proporcionalidad (minimización de datos).
  - Principios de exactitud y pertinencia (limitación a la finalidad de su recogida).
  - Principio de temporalidad (limitación del plazo de conservación).
  - Principios de licitud.
  - Principio de integridad y confidencialidad.

*"¿Qué quiere decir que los datos sean lícitos?"*

A diferencia del enfoque actual, ya no se plantean excepciones al consentimiento, sino que se regulan bases jurídicas del tratamiento:

- El consentimiento del afectado.
- Relación contractual u obligación legal.
- Interés vital del interesado u otra persona.
- Interés público.
- Interés legítimo del responsable, que prevalezca sobre los derechos del interesado.

- **El consentimiento del interesado**: Cuestiones a tener en cuenta:

  - Cuando la base de legitimación del tratamiento sea el consentimiento, el responsable debe estar en condiciones de acreditarlo (registro de consentimiento).
  - A diferencia de la normativa vigente, el consentimiento prestado al amparo del RGPD debe ser inequívoco y positivo (implícito: rellenar formulario). Excepciones: Se requiere que el consentimiento sea **explícito** cuando suponga:
    - El tratamiento de datos de categorías especiales.
    - La adopción de decisiones automatizadas.
    - La posibilidad de realizar transferencias internacionales.
  - En ningún caso cabe el consentimiento tácito, por inactividad.
  - Se debe contar con un consentimiento diferenciado por finalidades (cláusulas de opt-in).
  - Incluso en aquellos casos en que no es necesario el consentimiento, es preciso que se informe al interesado.
  - El Proyecto de LOPD entiende que el consentimiento prestado por los mayores de 13 años es válido.

*"¿Qué ocurre con los tratamientos realizados sobre la base de un consentimiento tácito conforme a la normativa derogada?"*

- **Medios para el ejercicio de los derechos de los afectados**: Tal como prevé la normativa vigente, se debe permitir y facilitar el ejercicio de los derechos de los interesados. El RGPD amplía el catálogo de derechos y los medios para cumplir con su ejercicio:

  - **Acceso:** Se amplía la información que se debe proporcionar, semejante al deber de información. Posibilidad de requerir que entregue en formato digital.
  - **Rectificación**: Se impone la obligación de que se comunique a todos los destinatarios de los datos, la rectificación, supresión y limitación del tratamiento.
  - **Supresión (cancelación)**: Responde a la configuración jurisprudencial del "derecho al olvido", cuando concurra justa causa.
  - **Oposición**: Se mantiene su configuración (oposición a los tratamientos basados en el interés legítimo, mercadotecnia y elaboración de perfiles).
  - **Limitación del tratamiento**: Derecho de nueva configuración, que supone la paralización del tratamiento cuando:
    - Ejercitada rectificación u oposición, mientras se resuelve la solicitud.
    - Proceda la supresión, pero se precisen los datos para el futuro.
  - **Portabilidad**: Derecho a obtener en formato electrónico los datos que posee el responsable, e incluso de que se envíen directamente a un tercero. Requisitos: Tratamiento automatizado y basado en consentimiento o contrato.

- Deber de contar con medios fáciles, accesibles y gratuitos para atender los requerimientos en el plazo de 1 mes, incluso la denegación de ejercicio.

- **Medidas de seguridad que proporcionan un estándar de protección mínimo**: Sin perjuicio de la necesidad de que los responsables adopten aquellas medidas que resultan adecuadas y proporcionales a los riesgos de su actividad, podemos identificar ciertas medidas que deberán adoptar todos los responsables:

  - Medidas de seguridad físicas y lógicas.
  - Seudonimización y confidencialidad de los datos.
  - Integridad, disponibilidad y resiliencia: recuperación y anticipación a las amenazas, así como la reducción de la dependencia de factores externos a la empresa.
  - Formación y concienciación de los empleados.
  - Copias de seguridad.
  - Auditorías: Verificación y evaluación de las medidas adoptadas.

- **Notificación de brechas de seguridad**: Deber de **documentar** y **notificar** las **violaciones de seguridad** a la **autoridad de control** competente sin demora injustificada y en un plazo máximo de 72 horas desde que tenga constancia, a menos que sea improbable que la violación constituya un riesgo para los derechos y libertades de los interesados. Además, se deberá **notificar las violaciones a los interesados**, cuando suponga un alto riesgo para los datos, salvo que los datos sean ininteligibles (e.g., cifrados) o se han tomado medidas posteriores.

- Si la notificación individual a los interesados supone una labor desproporcionada, se puede optar por una comunicación pública.

- **Realización de Evaluación de Impacto:** Antes de llevar a cabo cualquier tratamiento que probablemente suponga un alto riesgo para los derechos y libertades de los interesados, el responsable debe evaluar el impacto de las operaciones de tratamiento. Es obligatoria en los siguientes casos:

  - Evaluación sistemática y exhaustiva de aspectos personales basada en un tratamiento automatizado, a partir de la cual se toman decisiones que producen efectos jurídicos en relación con los particulares o les afectan significativamente.
  - Tratamiento a gran escala de categorías especiales de datos, o de datos relativos a las condenas penales y delitos.
  - Observación sistemática a gran escala de una zona de acceso público.
  - Los determinados por la autoridad de control, que comunicará al CEPD.

- **Consulta previa:** Si la evaluación de impacto indica que el tratamiento entraña un riesgo elevado, el responsable deberá consultar a la autoridad de control antes de proceder al tratamiento. Si la autoridad considera que el tratamiento no es conforme, deberá asesorar al responsable en el plazo máximo de 8 semanas, prorrogables otras 6 semanas.

"¿Qué es un Delegado de Protección de Datos?"

- Estatuto jurídico: interno y externo, relación laboral o mercantil.
- Certificación voluntaria, pero debe tener conocimiento de la legislación en materia a de protección de datos y comprensión de los sistemas de información y seguridad
- Puede desempeñar otro cargo (compliance officer), evitando los conflictos de interés (alta dirección)
- Funciones:

  - ❖ Informar y asesorar al responsable en materia de protección de datos.
  - ❖ Supervisar el cumplimiento de la normativa : formación del personal, auditorías, concienciación.
  - ❖ Cooperar con las autoridades de control.

*"¿Necesita mi empresa nombrar un DPO?"*

- Designación obligatoria cuando:

  - ❖ El tratamiento sea llevado a cabo por una autoridad u organismo público
  - ❖ La actividad principal del responsable o encargado consista en operaciones que requieran la observación habitual de interesados a gran escala.
  - ❖ La actividad principal de la empresa consista en el tratamiento de datos de categorías especiales a gran escala.

❑ El Proyecto de LOPD recoge situaciones concretas en las que es necesario nombrar un DPO.

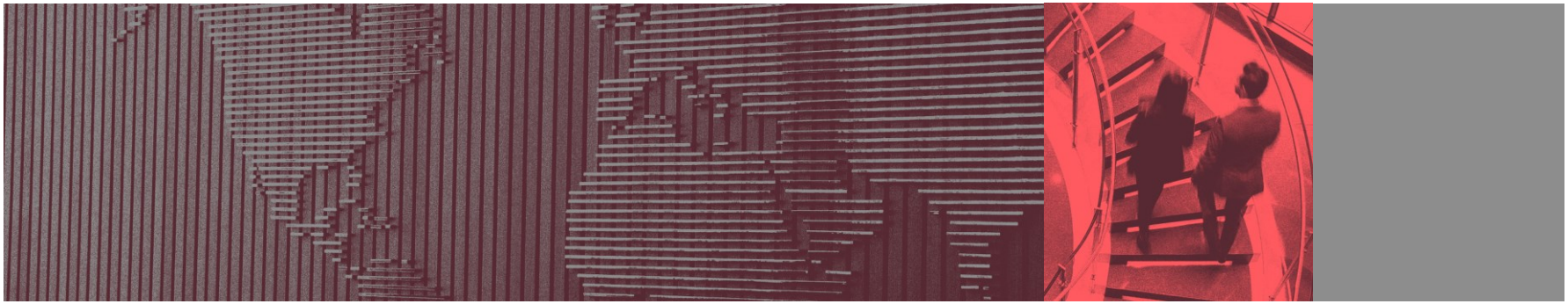
*"En resumen, ¿qué medidas debo adoptar para adaptarme a la normativa?"*

- Medidas legales:
  - ❖ Actualización de cláusulas informativas (doble capa).
  - ❖ Análisis de las bases legitimadoras de los tratamientos realizados.
  - ❖ Implantación de mecanismos de obtención del consentimiento expreso.
  - ❖ Adaptación de los contratos con los encargados de tratamiento.
- Medidas organizativas:
  - ❖ Elaboración de un procedimiento de notificación de brechas.
  - ❖ Actualización de protocolos de atención a los derechos.
  - ❖ Designación de un DPO.
  - ❖ Posible certificación y adhesión a códigos de conducta.
- Medidas de seguridad:
  - ❖ Adopción de medidas lógicas, físicas y organizativas adaptadas a la actividad.
  - ❖ Concienciación y formación de los empleados.

❑ Herramienta FACILITA RGPD, para empresas que realicen tratamientos de riesgo bajo.

CUATRECASAS

CEEI ELCHE
CENTROS EUROPEOS DE EMPRESAS INNOVADORAS



**MUCHAS GRACIAS**

Javier Aliño Sehwerert – javierjesus.aliño@cuatrecasas.com