EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS Y LA GESTION DE RECURSOS HUMANOS

Disposiciones finales del RGPD.

- El RGPD o (GDPR por sus siglas en Ingles) entró en vigor a los 20 días de su publicación en el DOUE. Será aplicable a partir de 2 años desde la fecha anterior.
- **“Es obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro”**
- Deroga la Directiva 95/46/CE y de facto la LOPD y el RDLOPD
- GT29 se convertirá en el Comité Europeo de Protección de Datos.

- Se revisará periódicamente. La Comisión remitirá informes al Parlamento y al Consejo cada 4 años. También propondrá modificaciones conforme a la evolución de las tecnologías de la información.
- España: Proyecto de Ley Orgánica de Protección de Datos 24-11-2017 en tramite parlamentario.

Resumen de las Novedades del RGPD

- ✓ Ámbito de aplicación
- ✓ Principios
- ✓ Nuevas categorías especiales de datos
- ✓ Consentimiento
- ✓ Menores
- ✓ Deber de información
- ✓ Derecho al Olvido
- ✓ Derecho a la portabilidad
- ✓ Registro de Actividades del tratamiento
- ✓ Encargado del tratamiento
- ✓ Evaluaciones de impacto relativas a la protección de datos
- ✓ Protección de datos desde el diseño y por defecto
- ✓ Códigos de conducta
- ✓ Delegado de protección de datos (DPD)
- ✓ Medidas de seguridad
- ✓ Notificación de violaciones de seguridad

Resumen de las Novedades del RGPD: Principios

- **El principio de “responsabilidad proactiva”:** necesidad de que el responsable del tratamiento aplique medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento.
- ¿Qué datos se tratan? ¿Con qué finalidad? ¿Qué tipo de operaciones? Demostrar que se cumplen las medidas.
- En síntesis, este principio exige una actitud consciente, diligente y proactiva por parte de las organizaciones frente a todos los tratamientos de datos personales que lleven a cabo.
- “**Enfoque de riesgo”:** las medidas a aplicar deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como el riesgo para los derechos y libertades de las personas.
- se deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como el riesgo para los derechos y libertades de las personas.
- se deberán modular en función nivel y del riesgo para las libertades
- Grandes corporaciones y pequeñas modularán sus medidas en función del riesgo

Resumen de las Novedades del RGPD: Principios

- **Protección de datos desde el diseño:** a la hora de establecer los medios para el tratamiento y durante el tratamiento, el responsable debe establecer medidas adecuadas para adecuarlo al RGPD y proteger los derechos de los interesados.

- **Protección de datos por defecto**: el responsable debe establecer medidas para garantizar que, por defecto, se traten únicamente los datos necesarios para los fines específicos del tratamiento. Afecta a:

  - la cantidad de datos recopilados,
  - al alcance del tratamiento,
  - al periodo de conservación
  - y a la accesibilidad (por defecto, los datos no pueden hacerse accesibles a un número indeterminado de personas sin intervención de la persona).

Resumen de las Novedades del RGPD: Ámbito Territorial

- El tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la UE, independientemente de que el tratamiento tenga lugar en la UE o no.

- El tratamiento de datos personales de residentes en la UE por parte de un responsable o encargado no establecido en la UE, cuando las actividades de tratamiento estén relacionadas con:
  - La oferta de bienes o servicios a residentes en la UE.
  - El control de su conducta, en la medida en que esta tenga lugar en la UE.
  - Obligación de designar por escrito un representante en uno de los Estados miembros en los que residan los interesados afectados por el tratamiento.

Resumen de las Novedades del RGPD: CONSENTIMIENTO

Consentimiento

- Entendido como declaración inequívoca o una acción afirmativa clara.
- Olviden las casillas ya marcadas, el consentimiento tácito o la inacción no constituirán un consentimiento válido.
- Lenguaje claro y sencillo con fácil acceso.
- Se podrá retirar en cualquier momento.
- Responsables que realizan tratamientos basados en ese consentimiento por omisión deberían evitar seguir obteniendo esta modalidad de consentimiento y revisar esos tratamientos de forma que a partir de mayo de 2018 se hayan adecuado a las previsiones del RGPD

Explicito cuando:

- Tratamiento de categorías especiales de datos
- Adopción de decisiones automatizadas
- Transferencias internacionales

Resumen de las Novedades del RGPD: CONSENTIMIENTO

Consentimiento en el ámbito laboral.

- En el ámbito laboral la formula del consentimiento deja de tener peso.

- No hay posición de igualdad (Grupo de trabajo art. 29)

- Se sustituye por el interés legitimo,

- El cumplimiento de las ley y la ejecución del contrato.

Resumen de las Novedades del RGPD: Deber de información

En el momento de recogida/obtención de los datos debe informarse de:

- 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, indicando existencia o ausencia de decisión de adecuación de la Comisión, o referencia a las garantías adecuadas y forma de obtener una copia.
- Plazo de conservación o, si no es posible, criterios para determinar el plazo.
- Derechos de acceso, rectificación, supresión, oposición, limitación y portabilidad. Si la base del tratamiento es el consentimiento, derecho a retirarlo en cualquier momento.
- 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.
- Existencia de un mecanismo de decisión automatizado que comprenda la elaboración de perfiles indicando la lógica aplicada y la relevancia y consecuencias previstas del tratamiento.

Resumen de las Novedades del RGPD: Portabilidad

Derecho a la portabilidad

- derecho de acceso en formato estructurado, de uso común y de lectura mecánica,
- Derecho a solicitar la transmisión a otro responsable
- basado en consentimiento
- Tratamiento Automatizado
- Datos propios, no de terceros.

El ejercicio debe ser sencillos, visibles y gratuitos: 1 mes + 2 en caso de ser complejas a notificar en 1 mes.

Resumen de las Novedades del RGPD: EIPD

Evaluaciones de impacto relativas a la protección de datos

¿Cuando? tratamiento que probablemente suponga un alto riesgo para derechos y libertades.

- Elaboración de perfiles sobre cuya base se tomen decisiones que produzcan efectos jurídicos sobre los interesados o que les afecten significativamente de modo similar
- Tratamiento a gran escala de datos sensibles
- Observación sistemática a gran escala de una zona de acceso público (concepto jco. indeterminado).
- Listas de tratamientos susceptibles de DPIA

Contenido de la DPIA:

- 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;
- una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;
- una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado
- las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

Resumen de las Novedades del RGPD: EIPD

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, facilitándole la siguiente información:

- 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.

- Cualquier medida legislativa que guarde relación con el tratamiento de datos debe someterse igualmente a consulta de la autoridad de control por los Estados miembros.

Resumen de las Novedades del RGPD: Registro de Actividades del Tratamiento

El responsable debe llevar **un registro de las actividades de tratamiento**, en el que constarán:

- Nombre y datos de contacto de: responsable, corresponsable, 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.
- Plazos previstos para la supresión de las diferentes categorías de datos.
- Descripción general de las medidas de seguridad.

Resumen de las Novedades del RGPD: Registro de Actividades del Tratamiento

- El registro estará a disposición de la autoridad de control.

- **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.

- La gran mayoría de las empresas y organizaciones deberán establecer un Registro e Actividades del Tratamiento, pues bastará una de las tres características (la característica de no ocasional) para que no se aplique la excepción anterior.

Resumen de las Novedades del RGPD: DPO o DPD

Delegado de protección de datos (DPD)

Interno o externo

Obligatorio:

- Administraciones publicas (excepto Juzgados y tribunales)
- Cuando el tratamiento requiera la observación habitual y sistemática de interesados a gran escala.
- Cuando el tratamiento tenga por objeto categorías especiales de datos personales o datos relativos a condenas o infracciones penales.

Funciones:

- Informar y asesorar al responsable o al encargado y a los trabajadores sobre las obligaciones que impone la normativa de protección de datos.
- Supervisar el cumplimiento de la normativa.
- La designación debe hacerse publica + Datos de contacto + deberán ser comunicados a las autoridades de supervisión competentes.
- necesidad de que se relacione con el nivel superior de la dirección o la obligación de que el responsable o el encargado faciliten al DPD todos los recursos necesarios para desarrollar su actividad.
- Nombrado atendiendo a sus cualificaciones profesionales y en particular a su conocimiento de la legislación y la práctica de la protección de datos.

Resumen de las Novedades del RGPD: Medidas de Seguridad

Medidas de seguridad

- No sigue una tipología.
- Se determinarán según el riesgo.
- Requiere hacer un análisis de los riesgos.

¿Cómo y cuáles?

- Grandes empresas: Metodologías de análisis de riesgos. ENS o Magerit V3, ISO.
- Medianas y pequeñas empresas: con tratamientos de poca complejidad este análisis sería el resultado de una reflexión, mínimamente documentada, sobre las implicaciones de los tratamientos en los derechos y libertades de los interesados.

Resumen de las Novedades del RGPD: Violaciones de Seguridad

Notificación de violaciones de seguridad

- Si se produce una violación de la seguridad, el responsable debe notificarlo a la autoridad de control.
- Plazo máximo de 72 horas, a menos que sea improbable que constituya un riesgo para los derechos y libertades de las personas.

Alto Riesgo: Comunicarlo a las personas afectadas.

Excepciones:

- El responsable hubiera adoptado medidas de protección adecuadas, como que los datos no sean inteligibles para personas no autorizadas.
- Haya aplicado medidas ulteriores que garanticen que ya no existe la probabilidad de que se concrete el alto riesgo.
- Suponga un esfuerzo • desproporcionado.

¿Qué se comunica a la Autoridad de control?

- naturaleza de la violación, categorías de datos y de interesados afectados,
- medidas adoptadas por el responsable para solventar la quiebra
- y, si procede, las medidas aplicadas para paliar los posibles efectos negativos sobre los interesados.

Resumen de las Novedades del RGPD: Encargado del Tratamiento

Debe regularse por contrato (o acto jurídico equivalente), que deberá incluir:

- Objeto, duración, naturaleza y finalidad del tratamiento, categorías de interesados y de datos personales, obligaciones y derechos del responsable y del encargado.

- El responsable debe elegir un encargado que ofrezca **garantías suficientes.**

- Subencargados: previa autorización.

- Obligaciones del encargado:
  - Garantizar el compromiso de confidencialidad de las personas con acceso a datos.
  - Implementar medidas de seguridad y ayudar al responsable a garantizar el cumplimiento de las obligaciones relativas a seguridad de los datos.
  - Asistir al responsable para atender los derechos de los interesados.
  - Poner a disposición del responsable información para probar el cumplimiento de sus obligaciones y permitir auditorías.
  - Informar inmediatamente al responsable si entiende que una instrucción vulnera la normativa de protección de datos.
  - Notificar violaciones seguridad.
  - Registro de actividades de tratamiento en nombre del responsable.

Resumen de las Novedades del RGPD: Autoridades de Control

- Se establece la obligación de tener, como mínimo, una autoridad de control por cada EM.
- Su Competencia se limita a los tratamientos de datos en el ámbito de su territorio.
- Normas de competencia:
  - Será autoridad de control principal la correspondiente al único establecimiento / establecimiento principal del responsable / encargado. Es el único interlocutor en caso de tratamiento transfronterizo de datos (dentro UE).
  - En cualquier caso, competencia de cada autoridad de control respecto a reclamaciones presentadas por presuntas infracciones cometidas por un establecimiento situado en su EM o afecte "sustancialmente" a interesados situados en su EM → vis atractiva de la autoridad de control principal (art. 56.3).

Resumen de las Novedades del RGPD: Autoridades de Control

Actos administrativos que puede adoptar la autoridad de control:

- **Advertencia** (eventual infracción) y **amonestación** (infracción);
- **Órdenes**; y
- **Sanciones económicas:**
  - Hasta 10 millones de euros o hasta el 2% del volumen de negocios mundial total anual del ejercicio financiero anterior (el importe más elevado): obligaciones de responsable/encargado, de organismos de certificación y de autoridades de control.
  - Hasta 20 millones de euros o hasta el 4% del volumen de negocios (el importe más elevado): principios básicos, no atención de derechos, transferencias internacionales.
  - Hasta 20 millones de euros o hasta el 4% del volumen de negocios (el importe más elevado): Incumplimiento de resoluciones de autoridades de protección de datos.

Resumen de las Novedades del RGPD: Referencias al derecho laboral

Tratamiento en el ámbito laboral

- Los EM podrán, a través de disposiciones legislativas o de convenios colectivos, establecer normas más específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral,

- Incluirán medidas adecuadas y especificas para preservar la dignidad humana de los interesados así como sus intereses legítimos y sus derechos fundamentales, prestando especial atención a la transparencia del tratamiento, a la transferencia de los datos personales dentro de un grupo empresarial o de una unión de empresas dedicadas a una actividad económica conjunta y a los sistemas de supervisión en el lugar de trabajo.

- Cada Estado miembro notificará a la Comisión las disposiciones legales que adopte a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier modificación posterior de las mismas.

MUCHAS GRACIAS

¿PREGUNTAS?