ÍTACA
advanced analytics

audria
AUDITORIA • CONSULTORIA

Col·legi de Censors Jurats de Comptes de Catalunya = EL CØL·L3G1

Implicaciones para los auditores de la LOPD

4 de Julio de 2019
Sitges

Col·legi de Censors Jurats de Comptes de Catalunya = EL CØL·L3G1

Implicaciones para los auditores de la LOPD

Principales novedades en protección de datos

Guía de adaptación para empresas de auditoría

Implicaciones como auditor de terceros

Conclusiones

ÍTACA
advanced analytics

audria
AUDITORIA • CONSULTORIA

ÍTACA
advanced analytics

audria
AUDITORIA • CONSULTORIA

Col·legi de Censors Jurats de Comptes de Catalunya = EL CØL·L3G1

Principales novedades en protección de datos

Implicaciones para los auditores de la LOPD

Objetivos del reglamento

European data protection for the digital era

Better protection for personal data

Council of the European Union
General Secretariat

Clear consent required to process data

More and clearer information about processing

Limits on the use of automated processing of data to make decisions, for example in the case of 'profiling'

Right to move data from one service provider to another

Right to rectify and remove data, including the 'right to be forgotten' for data collected as a child

Easier access to personal data

Right to notification if data is compromised

Stricter safeguards for transfer of personal data outside the EU

Tratamiento lícito, leal y Transparente

Presentación del RGPD

11 Capítulos | **99 Artículos** | **173 Consideraciones**

Capítulo **I**	Disposiciones Generales	**4** artículos
Capítulo **II**	Principios	**7** artículos
Capítulo **III**	Derechos del interesado	**12** artículos
Capítulo **IV**	Responsable del tratamiento y encargado del tratamiento	**20** artículos
Capítulo **V**	Transferencias de datos personales a terceros países u organizaciones internacionales	**7** artículos
Capítulo **VI**	Autoridades de control independientes	**9** artículos
Capítulo **VII**	Cooperación y coherencia	**17** artículos
Capítulo **VIII**	Recursos, responsabilidad y sanciones	**8** artículos
Capítulo **IX**	Disposiciones relativas a situaciones específicas de tratamiento	**7** artículos
Capítulo **X**	Actos delegados y actos de ejecución	**2** artículos
Capítulo **XI**	Disposiciones finales	**6** artículos

Definiciones

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

Responsable del tratamiento

La persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento.

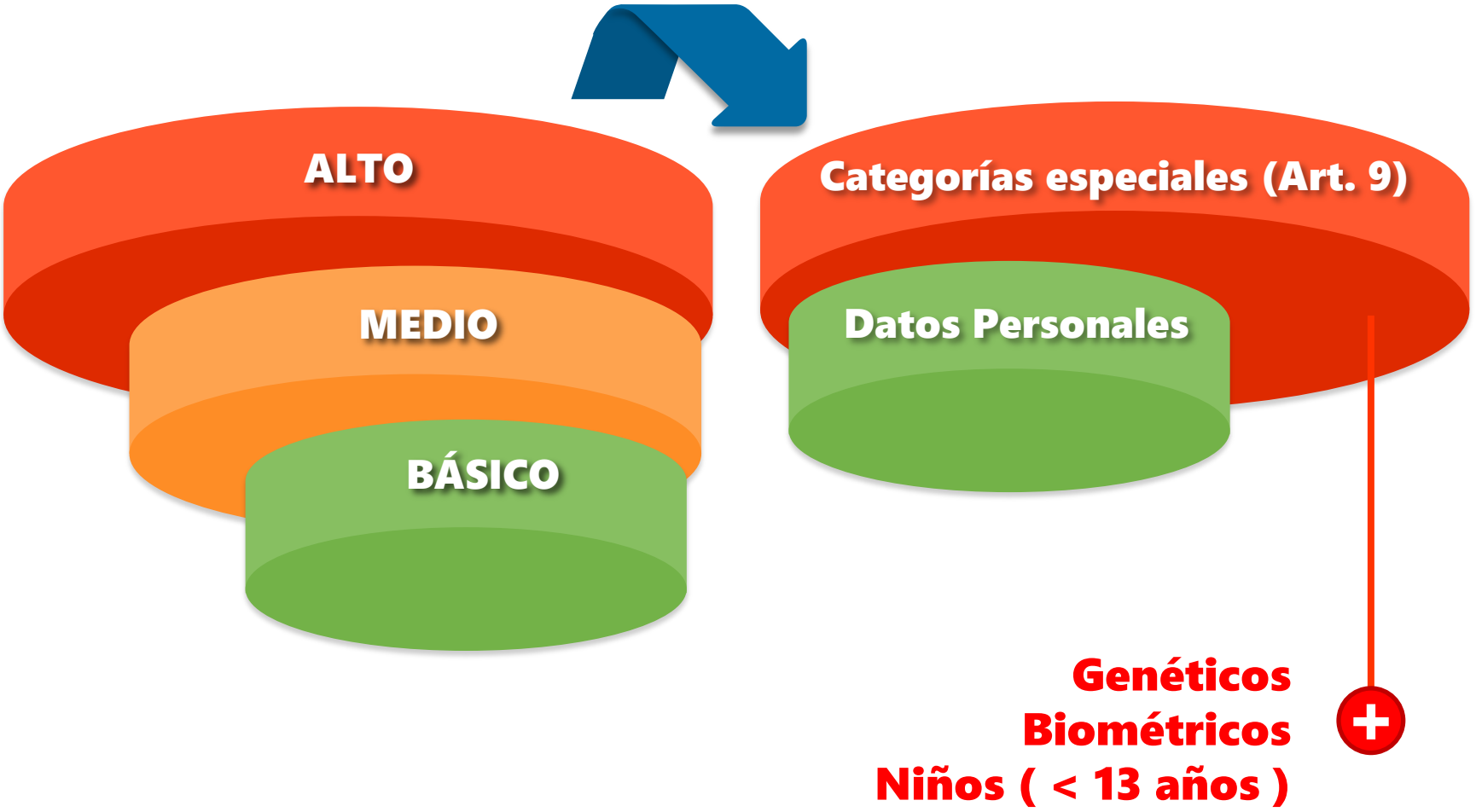
Encargado del tratamiento

La persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

Delegado de protección de datos

Responsable y asesor en materia de protección de datos de la compañía, sin responsabilidad jurídica.

Categorías de datos



Derechos del interesado

- **Desaparece el "consentimiento tácito".**
- **Comunicaciones:**

  En el momento de recogida de datos (directa o indirecta).
  Si cambia la finalidad.
  Si hay transferencia de datos a terceros países.

- **Derecho de acceso en cualquier momento (hasta el máximo detalle)**
- **Derecho a rectificación, oposición, olvido.**
- **Oposición a mercadotecnia directa o a la elaboración de perfiles.**
- **Derecho a oponerse a que se tomen decisiones automatizadas en base a sus DP.**

Obligaciones de las empresas

Catálogo de medidas del título VIII RLOPD → **Capítulo IV del RGPD (+ genérico)**

Responsabilidad pasiva	Responsabilidad proactiva
Enfoque cumplimiento	Enfoque riesgos
Notificación de ficheros	Documentar Tratamientos
Documento de Seguridad	PIAs
Responsable de Seguridad	Data Protection Officer
Códigos tipo	Códigos de conducta
Auditorías Bienales	Certificación

Nuevo régimen sancionador

Artículo 83 RGPD

Condiciones generales para la imposición de multas

"Sanciones efectivas, proporcionadas y disuasorias"

Sujetos responsables: Responsable del Tratamiento y encargado del tratamiento

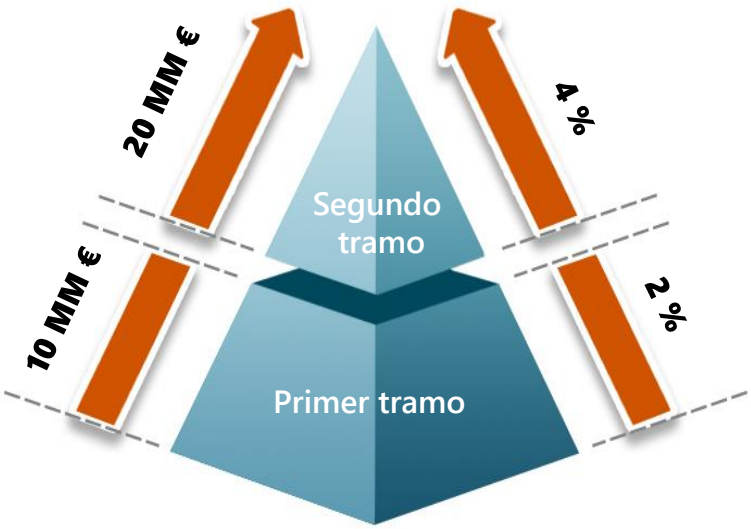
Aspectos a tener en cuenta:

- Naturaleza, gravedad y duración de la infracción.
- Intencionalidad o negligencia en la infracción.
- Medidas tomadas para paliar los daños prejuicios sufridos por los interesados.
- El grado de cooperación con la autoridad de control y si fue comunicada de forma previa a la denuncia.
- Adhesión al código de conducta.

Se puede sancionar aunque no haya habido un caso concreto.

Cuantía de las sanciones

Artículo 83 RGPD



Diferentes sanciones en función del sujeto infractor:

- **Personas físicas:** Multa pecuniaria directa.
- **Personas jurídico-privadas:** Multa pecuniaria directa, o porcentaje del volumen de negocios anual a nivel mundial con respecto al ejercicio anterior, en caso de que esta última cifra sea superior.
- **Personas jurídico-públicas:** Se deja abierta la posibilidad de que cada Estado Miembro pueda promulgar leyes que establezcan las sanciones correspondientes.

La nueva LOPD (trasposición española)

Art. 7 – Se establece la edad del consentimiento del menor en 14 años.

Art. 11 – Transparencia de la información, informar por "capas"

Art. 13 – Se introduce el concepto de sistema de acceso remoto para ejercer los derechos del interesado.

Art. 15 y 16 – Obligación de marcado en casos de limitación/supresión

Art. 23 – Sistema de exclusión publicitaria de obligatoria consulta.

Art. 24 – Regulación del canal de denuncias en cuanto a privacidad.

Art. 31 – Los organismos públicos están obligados a publicar sus tratamientos.

Art. 34 – Se amplía el rango de personas jurídicas que necesitan DPO.

Art. 72/73 y 74 – Se especifican las sanciones en muy graves, graves y leves.

Guía de adaptación para empresas de auditoría

Implicaciones para los auditores de la LOPD

Definición del alcance - RAT

¿Se han determinado las **actividades de tratamiento que hace la empresa?**

- Clientes
- Proveedores
- Candidatos
- Patrocinadores y colaboradores
- Asistentes a cursos, congresos y jornadas

Un fichero puede tener varios tratamientos

¿Se ha definido un **responsable** para cada tratamiento?

¿Se dispone de **categorías especiales** de datos? (salud, de menores, ideologías….)

Entender el flujo de información

¿Se conoce el flujo de información de los tratamientos?

- ¿Cómo se **recaba** la información?
- ¿Cuál es la **legitimación** del tratamiento?
  - Consentimiento
  - Ejecución de un contrato
  - Obligación legal
  - Interés legítimo
- ¿Durante cuánto tiempo se **conservan**?
- ¿Se **ceden** a terceros? ¿**Dónde se ubican** los terceros?
- ¿Se dispone de **encargados de tratamiento**?

Evaluación de riesgos (I)

¿Se han adaptado las **cláusulas** contractuales?

- Clientes
- Proveedores
- Empleados

¿Se ha adaptado la **página web**?

¿Se dispone de mecanismos para dar **respuesta a los derechos** de los interesados?

- Derecho a la información (cuando se recaba y en cualquier momento)
- Derecho a retirar el consentimiento
- Mecanismos para poder ejercer sus derechos (mail, etc.…
- Procedimientos internos de respuesta.

Evaluación de riesgos (II)

¿Se ha evaluado la necesidad de un **DPO**?

¿Se ha evaluado la necesidad de **PIAs**?

¿Qué medidas de **seguridad** se han implantado?

- Control de acceso
- Minimización de datos personales
- Anonimización
- Encripción
- Transferencias internacionales
- Detección y gestión de incidentes de seguridad

¿Se dispone de **códigos de conducta** sectoriales?

Aspectos relevantes

Concienciación y **formación** del personal involucrado.

Protección de datos desde el **diseño** y **por defecto**.

Control y gestión de los **proveedores** y **herramientas de trabajo/comunicación.**

ÍTACA
advanced analytics

audria
AUDITORIA · CONSULTORIA

Col·legi de Censors Jurats de Comptes de Catalunya = EL CØL·L3G1

Implicaciones como auditor de terceros

Riesgos para el auditor

- Riesgo de sanciones
- Daño reputacional
- Pérdida de confianza del mercado
- Violación de datos personales:
  - Brecha de seguridad que permita la destrucción, pérdida, alteración, divulgación no autorizada o acceso a datos personales.
  - Robo o pérdida de dispositivos.
  - Datos en soporte papel.

¿Cómo se audita el RGPD?

Análisis de Riesgos Protección de Datos Personales:

- Riesgo medio/bajo: n/a EIPD
  - Check list y procedimientos de auditoria
- Riesgo alto:
  - Expertise

¿Cómo se audita el RGPD?

Herramientas disponibles:

- Herramienta FACILITA de la AEPD
- Guías para realización de PIAs
- Check List de análisis de riesgos de la AEPD

Conclusiones

Conclusiones

- Toca trabajar con un enfoque **basado de riesgos** y en la **prevención activa**.
- La privacidad será un elemento más del "día a día" de nuestros productos y servicios, y no volverá a ser un "problema" estático, que se resuelve con unos procedimientos y una auditoría cada dos años.
- Se requerirán procedimientos nuevos (PIAs, comunicaciones, incidentes…) y una estructura organizativa nueva.
- Se establece la **formación** como un elemento clave, más orientada a la **concienciación**.
- Es una **evolución natural de la ley actual**, no una ruptura. La privacidad hace tiempo que se encuentra dentro de la cultura de las compañías, aunque tendremos que participar más activamente de ello.
- Se necesita guardar evidencia (poder demostrar) que se están aplicando las medidas adecuadas