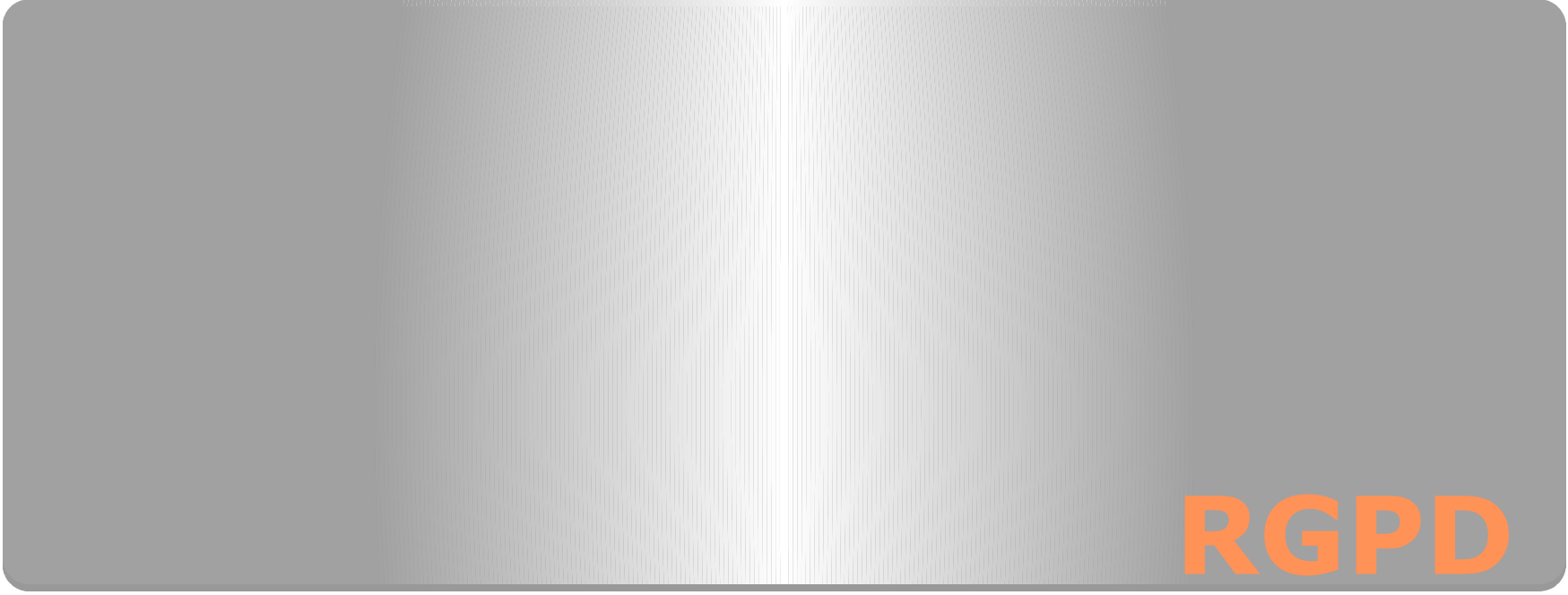




RGPD

Una guía para Pymes y profesionales

- El RGPD nace como nexo de unión de todas las LOPD a nivel europeo y nace con la vocación de convertirse en el único marco regulador sobre protección de datos en los países de la Unión Europea
- Este Reglamento, entró en vigor en mayo de 2016 pero no será de obligado cumplimiento hasta el 25 de mayo de 2018
- Como novedades, incorpora nuevas obligaciones y nuevas figuras profesionales, entre ellas la más importante es la del DPD, de la que hablaremos a lo largo de esta sesión

Introducción

Novedades del RGPD:



Derecho al **olvido**



Evaluación de **impacto**



Análisis de riesgo:
Listas de verificación



Notificación de
quiebras de seguridad



Sanciones e indemnizaciones



Figura del **DPD**

LGPD vs RGPD

- **¿Datos, ficheros, imágenes...?**



Unas preguntas...

- **¿Sabemos lo que es un dato?**

- Cualquier información numérica, alfabética, gráfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables

Unas preguntas...

- **¿Protegemos el dato? o ¿el contenido del dato?**
- **¿Qué o quién es el responsable del fichero?**
- **¿Qué o quién es el responsable del tratamiento de los datos?**

Unas preguntas...

● Contenidos

- Bases de legitimación
- Transparencia e información a los interesados
- Obligaciones y derechos de los interesados
- Responsable, Encargado y DPD
- Responsabilidad Activa
- Transferencias internacionales
- Tratamiento de datos de menores
- Sanciones

Aplicación del RGPD

- **Bases de Legitimación para el tratamiento de los datos**

- Consentimiento explícito e inequívoco
- Contrato entre las partes
- Intereses vitales (Hª clínica, datos salud,...)
- Deber de información
- Interés público

Con o Sin Consentimiento

- **Transparencia e información a los interesados**

¿Por qué y para qué queremos sus datos?

- Información Clara/Concreta/Concisa
- Basada en qué términos legales
- Nombre del **Responsable/DPD** del fichero
- Si se harán transferencias internacionales

Solicitud de datos

- **Obligaciones y Derechos de los Interesados**

Antes del RGPD	Con el RGPD
Debían facilitarse todos los datos de base del afectado, pero no copias o documentos (excepto en el caso de la historia clínica).	Se reconoce el derecho a obtener una copia de los datos personales objeto del tratamiento.

Solicitud de datos

- **Derechos del ciudadano en la Cesión y Acceso a los datos**



Ciudadano

◦ ARCO-O



Acceso



Rectificación



Cancelación



Oposición



Olvido

Derecho de Acceso a los Datos

Derechos de la empresa para el tratamiento de datos

- **Solicitar datos** al interesado de manera informada y según el reglamento
- **Uso de los datos** según Reglamento
- **Solicitar remuneración Si:**
 - La petición es reiterativa
 - La petición no esté fundamentada o sea improcedente

Derechos de la Empresa

Obligaciones de la empresa



Registro de las Bases de datos



Establecer un modelo y
documento de seguridad



Facilitar el ejercicio de los
derechos de los interesados



Designar personal para la
Protección de Datos

Obligaciones de la Empresa

● **Nuevas figuras profesionales**

- Nexo de unión entre ciudadano/empresa y empresa/AEPD
- Nuevas funciones
- Garantizan el principio de responsabilidad activa
- Responsable, Encargado y DPD

Profesionalización de PD

DPD

- **Supervisa** a Encargado/Responsable
- **Auditorías y Simulacros** anuales
- **Obligatorio** según tamaño empresa y tipo de datos
- Debe **identificarse** en todas las **comunicaciones**

Responsable

- **Supervisa** el registro de datos
- **Determina** las medidas de **copia y Sistema de Seguridad**
- Designa DPD y Encargado

Encargado

- Lleva el **Registro de cambios**
- Ejecuta **medidas y copias de seguridad**
- **Informa** a Responsable y/o DPD

Profesionalización de PD

● Delegado de Protección de Datos o DPD

- Profesional auditado y **certificado**
- Profesional **independiente** de la empresa
- Es figura de **autoridad** sobre Responsable y encargado
- Responsable de **Auditorías, control de la seguridad y de los simulacros**
- Obligatorio en:
 - **Empresas con tratamiento de datos sensibles** (judiciales, penales...)
 - Empresas de más de 250 empleados
 - Administraciones Públicas

Profesionalización de PD

● Responsabilidad activa

1. Evaluación de Impacto sobre la Protección de datos EIPD
2. Análisis de riesgo
3. Medidas de Seguridad
4. Registro de actividades
5. Notificación de “quiebras de seguridad”

Responsabilidad Activa

1. Evaluación de Impacto sobre la Protección de datos EIPD

- Revisar **datos de alto riesgo** para derechos y libertades
- **Documentar todas las EIPD.** Al menos una Evaluación por cada tratamiento de datos
- Consultar a la AEPD sobre el procedimiento a seguir en casos de **coste inasumible causados por el tratamiento**

Responsabilidad Activa

2. Análisis de riesgo

- Informe sobre todo el ciclo del tratamiento y la **posibilidad de riesgo de pérdida de derechos y de datos** del interesado
 - Origen de los datos
 - Tratamiento de los datos
 - Finalización del tratamiento
 - Borrado de datos

Responsabilidad Activa

3. Medidas de Seguridad

- Activas

- Control de acceso (usuario y contraseña)
- Prohibición de guardar material ajeno en equipos de la empresa
- Acceso controlado al servidor/es
- Acceso controlado al archivo
- Protocolo de uso de la información en papel

- Pasivas

- Servidor de datos dedicado (usuario y contraseña)
- Copia de seguridad instantánea en servidor o disco externo
- Copia de seguridad remota encriptada

Responsabilidad Activa

4.Registro de actividades

- Modificación/cambio
 - Dato original /modificado
 - Fecha y hora de la modificación
 - Usuario que modifica
 - Autorización o solicitud (derechos ARCO)
- Borrado
 - Fecha y hora del borrado
 - Usuario que borra
 - Autorización o solicitud (derechos ARCO)

Responsabilidad Activa

5. Notificación de “quiebras de seguridad”

- Procedimiento
 - **Notificar a la AEPD** si se supone riesgo de derechos y libertades
 - Plazo máximo **72 horas** desde la quiebra
 - **Datos de interés:**
 - Naturaleza de la quiebra
 - Categorías de datos e interesados afectados
 - Medidas correctivas adoptadas para
 - Solventar la quiebra
 - Para paliar efectos negativos sobre los interesados

Responsabilidad Activa

● Transferencias Internacionales

- Transmisión de datos **fuera del territorio** del Espacio Económico Europeo
 - Cesión o comunicación de datos
 - Tratamiento de datos por el Responsable del fichero
- Precisa de **autorización expresa y explícita**

Otros tratamientos

- **Tratamiento de datos de menores**

CONSENTIMIENTO

De padres o tutores hasta los 15

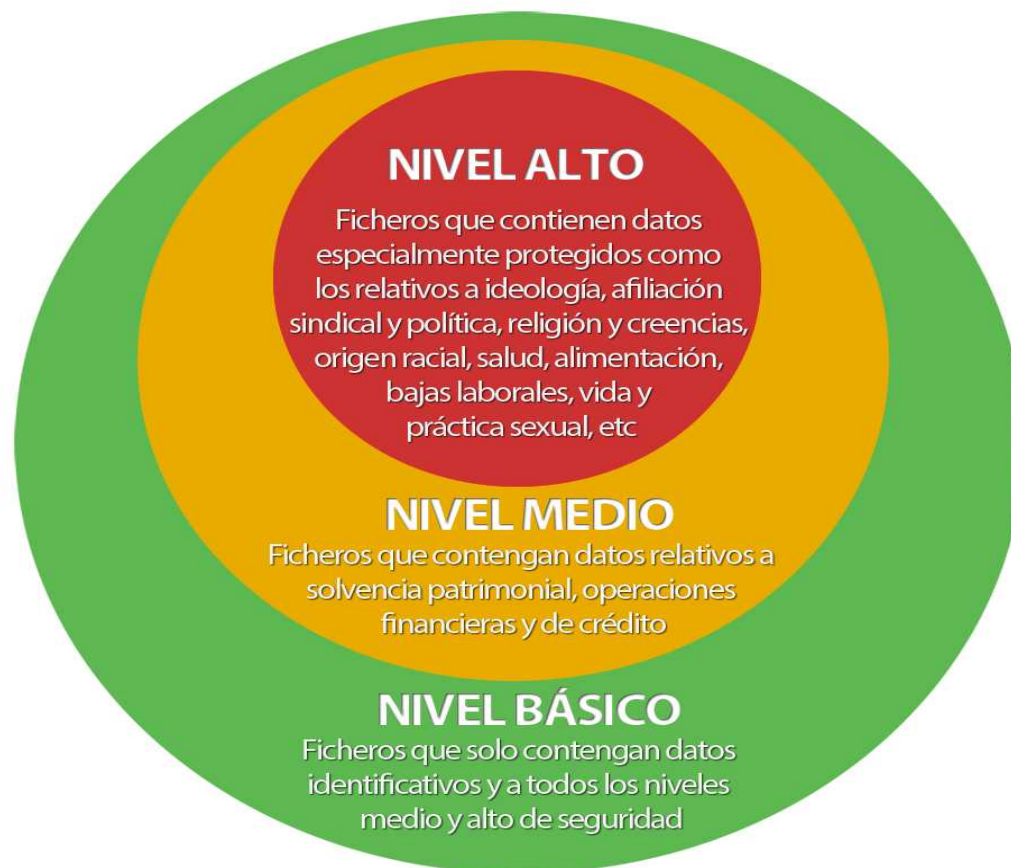
Del menor desde los 16

Cada estado miembro indica una edad de consentimiento.

Datos se refiere a **datos personales e imágenes**

Otros tratamientos

● Niveles de Seguridad de los datos



Seguridad e incumplimiento

iii Especial atención!!!

Nivel de seguridad Alto

Datos especialmente protegidos

Seguridad e incumplimiento

Sanciones

Leves

Graves

Muy Graves

Indemnizaciones (novedad en el RGPD)

Incumplimiento

NIVEL ALTO

Ideología, religión, creencias, origen racial, salud...

Infracción Muy Grave (300.506€ a 601.001€)

NIVEL MEDIO

Información penal, administrativa, hacienda pública...

Infracción Grave (40.001€ a 300.506€)

NIVEL BASICO

Datos personales (Nombre, apellidos, teléfono, direcciones de contacto...)

Infracción Leve (901€ A 40.000€)

Incumplimiento de la LOPD

● Web de la Agencia Española de Protección de Datos

- <http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion>
- <https://www.boe.es/doue/2016/119/L00001-00088.pdf>
- **Ley Orgánica 15/1999**, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- **Real Decreto 1720/2007**, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- **Instrucción 1/2006**, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.
- **Instrucción 1/1996**, de 1 de marzo, de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios.
- Hay mucho mas: preguntanos info@exploradigital.es

Bibliografía

- La propiedad intelectual de este curso pertenece a Explora Digital 2016, S.L

- Ponente y textos: Ángel Rodríguez Ruiz
- Diseño de la presentación y Textos: Elena Pérez Llano
- Diseño de Gráficos: Jaime Ascaso

- <https://exploradigital.es/>

-  @ExploraDigital

-  @ExploraDigital

Un curso de Explora Digital