ENTENDER
EL NUEVO MARCO LEGAL

Fernando Cuatrecasas

7 de Noviembre de 2017

REGLAMENTO UE 2016/679, DE 27-4-2016

- Protección de las personas físicas – tratamientos datos personales y la libre circulación de éstos
- Dº Fundamental
  - Carta de los D. Fundamentales de la UE (Art.8.1)
  - Tratado de Funcionamiento de la UE (Art.16.1)
  - Constitución Española (Arts. 10 y 18.4)
- Aplicación directa
- Aplicación a partir del 25 de mayo de 2018
- Deroga Directiva 95/46/CE – LOPD 15/1999 y RD 1720/2007
- Nueva LOPD en España- Primavera 2018

- **Unifica** marco normativo europeo
- Nivel uniforme y **más elevado de protección**
- Eliminar fragmentación y obstáculos libre circulación
- Evolución tecnología y globalización – Incr. Flujos transfronterizos
- Muchos más datos, más accesibles, más actores, más fáciles de procesar & Más difícil control sobre uso y destino
- Refuerza **seguridad jurídica y transparencia**
- Refuerza **Dºs de los interesados** (Olvido, Portabilidad…)
- Refuerza **Obligaciones de las empresas** (Res. Trat.-Enc. Trat)
- Nuevo régimen sancionador **– endurece sanciones**

- No sólo cambio legislativo, es un **CAMBIO DE MODELO**
- Instaurar Protección Datos como **CULTURA**, no sólo obligación
- Cultura de **cumplimiento, control, ética, de gestión de riesgos.**
- **"El Estado toma el timón y deja a la sociedad remar"**
- "Autorregulación"
- Quien mejor que la **propia empresa** para determinar sus **riesgos** y para tratar de **poner solución (medidas)**

Proyecto corporativo Compliance Protección de Datos

Para todas las empresas

Se protege bienes jurídicos con independencia del tamaño

Mayor compromiso por parte de la Entidad

Control del cumplimiento

PRINCIPIO de RESPONSABILIDAD ACTIVA

ENFOQUE DE RIESGO

RÉGIMEN SANCIONADOR ADMINISTRATIVO Y PENAL

1- Cultura de cumplimiento, control, ética

2 - Establecimiento de objetivos

3 -Identificar RIESGOS de incumplimiento

Revisar procesos
¿Para que uso datos? ¿Quien tiene acceso dentro y fuera

4- Valorar RIESGOS

Probabilidad / Gravedad
ISO 31000

5 -Determinar y aplicar MEDIDAS TÉCNICAS Y ORGANIZATIVAS EFICACES

-Prevenir riesgos y cumplir normativa
Garantizar nivel de seguridad adecuado al riesgo

Privacidad en el diseño
Privacidad por defecto
Evaluación del impacto
Consulta previa

6- Registro de actividades de tratamiento

7 - Notificación violaciones de seguridad

8 - Controlar / Supervisar

Delegado Protección Datos
Obligatorio / Voluntario
Interno /externo
P. Física / P. Jurídica

9 -Demostración del cumplimiento

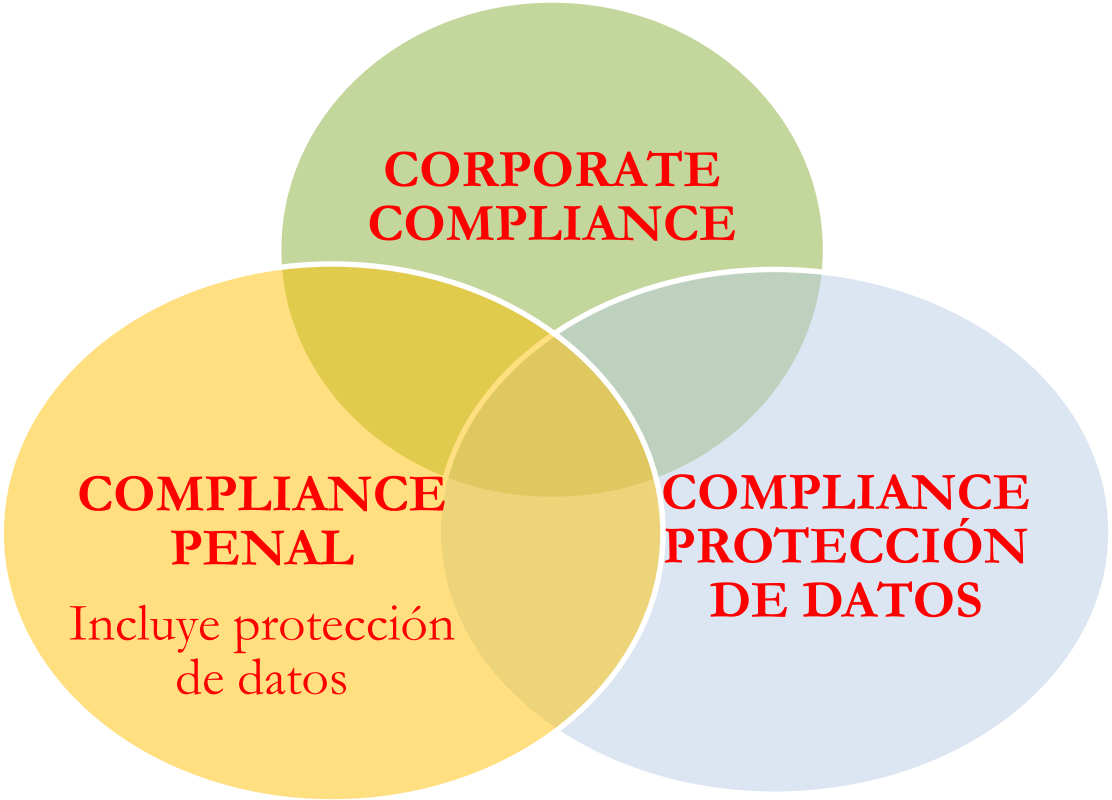
Adhesión Cód. de Conducta
Certificación

COMPLIANCE NO SÓLO ADMINISTRATIVO, TAMBIÉN PENAL

- **Responsabilidad penal de la P. Jurídica – Reformas Código Penal - LO 5/2010 y LO 1/2015**
- **Programa de Compliance Prevención Delitos – Exención de la R. Penal**
- **Delitos contra la privacidad de los datos personales conllevan R. Penal de la P. Jurídica (Art 197 Código Penal)**
- **Delito : Acceder, apoderarse, utilizar, modificar o alterar, ceder datos reservados de carácter personal o familiar.**
- **Régimen sancionador penal, además del administrativo.**

-Multa, prohibición o suspensión actividades, clausura locales, inhabilitación para obtener subvenciones o ayudas públicas, inhabilitación para contratar con el sector público o gozar de beneficios fiscales o de la S.S, intervención judicial, disolución-

Protección Datos y Compliance - "Juntos y revueltos"



ENTENDER
EL NUEVO MARCO LEGAL

Marc Querol

7 de Noviembre de 2017

ÍNDICE

INTRODUCCIÓN

25 de mayo de 2018

Ley Orgánica de Protección de datos 15/1999

Nueva Ley Orgánica de Protección de Datos (pendiente aprobación)

~~**Reglamento de desarrollo de la LOPD (RD 1720/2007)**~~

Reglamento General de Protección de Datos (RGPD)

INTRODUCCIÓN II

La principal ventaja del RGPD es la homogenización de obligaciones, es decir, las empresas deberán llevar a cabo acciones parecidas en todos los Estados miembros.

La uniformidad no será total, razón por la que en España se aprobará una nueva LOPD que regule aspectos concretos.

FICHEROS Y NIVELES DE SEGURODAD

EVALUACIONES DE IMPACTO

Se deberán realizar evaluaciones de impacto en materia de protección de datos: será necesario analizar riesgos e implantar mecanismos y procedimientos para proteger la información en función de la criticidad de los datos tratados y de las consecuencias de que terceros no autorizados accedieran a dichos datos.

PRIVACIDAD EN EL DISEÑO Y PRIVACIDAD POR DEFECTO

La **privacidad en el diseño** busca que las empresas intenten evitar invasiones en la privacidad durante el diseño y desarrollo de sus productos, procesos o servicios.

La **privacidad por defecto** pretende garantizar que, por defecto, sólo sean objeto de tratamiento los datos personales necesarios para el fin perseguido.

INFORMACIÓN AL AFECTADO

La información que se deberá dar a los afectados será mucho más extensa que en la actualidad

- Identidad y datos de contacto del responsable
- Datos de contacto del delegado de protección de datos (si aplica)
- Fines del tratamiento y base jurídica del mismo
- Destinatarios de los datos
- Intención de transferir datos a otro país
- Plazo de conservación o, cuando no sea posible, los criterios para determinar el plazo
- Los derechos del afectado
- El derecho a presentar una reclamación ante una autoridad de control
- Si la comunicación de datos es un requisito legal o contractual y las consecuencias de no facilitarlos
- La existencia de decisiones automatizadas, incluida la elaboración de perfiles, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado

FORMA DE RECABAR EL CONSENTIMIENTO

Se verá modificada la figura del consentimiento.

El consentimiento será toda manifestación de voluntad libre, específica, informada que conlleve una aceptación inequívoca del usuario, ya sea mediante una declaración o a través de una acción afirmativa

Los silencios y las casillas premarcadas no serán formas válidas de obtención de consentimiento.

FORMA DE RECABAR EL CONSENTIMIENTO

Se verá modificada la figura del consentimiento.

El consentimiento será toda manifestación de voluntad libre, específica, informada que conlleve una aceptación inequívoca del usuario, ya sea mediante una declaración o a través de una acción afirmativa

Los silencios y las casillas premarcadas no serán formas válidas de obtención de consentimiento.

DERECHO DE LOS AFECTADOS

Derecho de acceso, rectificación y oposición

Derecho de supresión (“el derecho al olvido”)

Derecho a la limitación del tratamiento

Derecho a la portabilidad de los datos

***Derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado**

NOTIFICACIÓN DE BRECHAS DE SEGURIDAD

Obligación de notificar a las autoridades de protección de datos las violaciones de seguridad en un plazo máximo de 72 horas y a las personas afectadas, en determinados supuestos y sin demora injustificada.

DATA PROTECTION OFFICER

Funciones del DPO:

- Informar y asesorar a la empresa y a sus empleados en relación a las obligaciones que les incumben según el Reglamento
- Supervisar el cumplimiento del Reglamento, y otras disposiciones de protección de datos
- Asesorar en los casos de evaluaciones de impacto y supervisar su aplicación
- Cooperar con la autoridad de control

Obligatorio para:

- Autoridades u organismos públicos
- Entidades cuyas operaciones de tratamiento requieran una observación habitual y sistemática de interesados a gran escala
- Entidades que realicen tratamientos a gran escala de categorías especiales de datos

VENTANILLA UNICA

Introducción de la ventanilla única, que permitirá a cualquier ciudadano presentar una reclamación ante la autoridad de protección de datos de su lugar de residencia, de su lugar de trabajo o del lugar donde se hubiera cometida la presunta infracción, independientemente del domicilio de la sede de la empresa denunciada

INCREMENTO DE SANCIONES

Las multas podrán ascender a

- 20 millones de euros, o

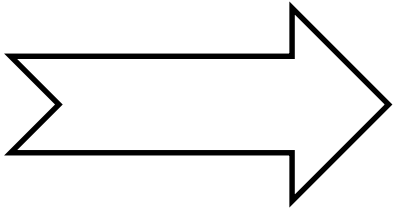
- al 4% de la facturación mundial anual de la empresa (o grupo de empresas).

CONCLUSIONES

Cambio de paradigma

Objetividad

Adopción de medidas concretas (RD 1720/2007)



Subjetividad

Adopción de **medidas de seguridad eficaces** (a discreción)

Una correcta gestión de la seguridad de la información será clave para poder cumplir con la normativa de protección de datos.

Será muy conveniente contar con *partners* tecnológicos de confianza.

LOGICALIS

Business and technology working as one

Gracias