QAEC

Insight exclusivo AEC

Descubre las claves de la nueva figura del Delegado de Protección de Datos DPD / DPO

Insight exclusivo AEC

Descubre las claves de la nueva figura del Delegado de Protección de Datos DPD / DPO

16 de noviembre de 2017

Eduard Chaveli

Socio – General Manager & Legal Services Director en Govertis

Organiza

AEC
ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

Con la colaboración de

GOVERTIS
Advisory Services

NUEVO MARCO NORMATIVO

- **RGPD.** Deroga la Directiva 95/46/CE.
- Intento de **armonizar u homogeneizar la normativa**
- Entró en vigor el 24 de mayo de 2016.
- Efecto directo. **No requiere trasposición al derecho interno.**
- **Será exigible a partir del 25 de mayo de 2018.**
- **Hasta la fecha deberemos realizar una adaptación progresiva.**
- **Nueva LOPD**. Actualmente existe un proyecto **(NLOPD)**

GRAN TRABAJO DE LAS AUTORIDADES DE CONTROL

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

La AEPD presenta en su 9ª Sesión Anual Abierta recursos y directrices para facilitar que las pymes cumplan con el Reglamento

La Agencia muestra la versión en pruebas de una herramienta de ayuda dirigida a empresas que tratan datos personales con escaso nivel de riesgo. Este recurso se ha ofrecido a asociaciones empresariales y colegios profesionales para que aporten sugerencias.

9ª sesión anual

European Commission

ARTICLE 29
Data Protection Working Party

apdcat
Autoritat Catalana de Protecció de Dades

DIRECTRICES PARA LA ELABORACIÓN DE CONTRATOS ENTRE RESPONSABLES Y ENCARGADOS DEL TRATAMIENTO

GUÍA PARA EL CUMPLIMIENTO DEL DEBER DE INFORMAR

Datuak Babesteko Euskal Bulegoa
Agencia Vasca de Protección de Datos

PRINCIPALES NOVEDADES Y OBLIGACIONES

- ✓Ampliación ámbito territorial de aplicación
- ✓Viejos y nuevos conceptos
- ✓Viejos y nuevos principios
- ✓El tratamiento como protagonista
- ✓El registro de las actividades de tratamiento
- ✓Cambios en los derechos del titular de los datos
- ✓Cambio en el enfoque de las medidas de seguridad
- ✓Evaluaciones de impacto
- ✓Cambios en las reglas de licitud del tratamiento.
- ✓Cambios en el deber de información
- ✓Nueva figura del delegado de protección de datos
- ✓Diferente régimen sancionador
- ✓Autoridades de control

COMPARATIVA LOPD/RGPD

Notificación e inscripción de ficheros al RGPD	Registro de Actividades de Tratamiento + medidas
Deber de información	Cambios en deber de información
Legitimación del tratamiento y reglas consentimiento.	Cambios en legitimación, consentimiento y menores.
Contratos con encargados del tratamiento	Cambios en los contratos de encargo de tratamiento
Derechos A.R.C.O.	ARCO + Limitación + portabilidad y Derecho olvido
Documento de seguridad e implantación de medidas de seguridad de carácter técnico y organizativo en el sistema de información.	Responsabilidad proactiva: • Medidas documentadas pero no DS • Notificación violaciones de seguridad • Privacidad desde el diseño y por defecto • Evaluaciones de Impacto en la Privacidad (EIPD) • Accontability • **DPO**
Formación a Responsables de Seguridad. Concienciación a usuarios	Además de usuarios y responsables a DPO
Auditoria bienal de las medidas de seguridad	Auditorias cuando determine el responsable

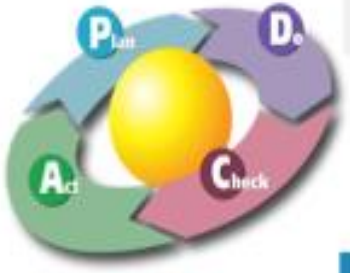
HOJA DE RUTA: UN PDCA DEL RGPD

FASE - PLAN

- Definición de responsables. DPO/CSO etc...
- Inventario de tratamientos
- Análisis de necesidad/ conveniencia EIPD
- Realización de EIPD (con funciones de Plan de tratamiento)

FASE - DO

- Implantación de controles:
  - Jurídicos (Cláusulas, Contratos)
  - Técnicos (Medidas de Seguridad)
  - Organizativos (Procedimientos diversos)
- Formación
- Registro de actividades de tratamiento



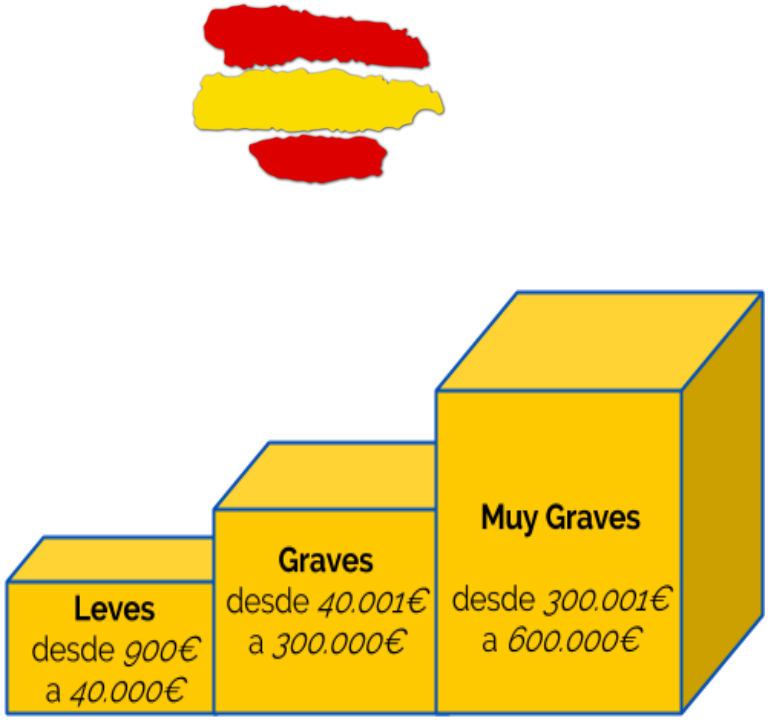
FASE - REVISIÓN (CHECK)

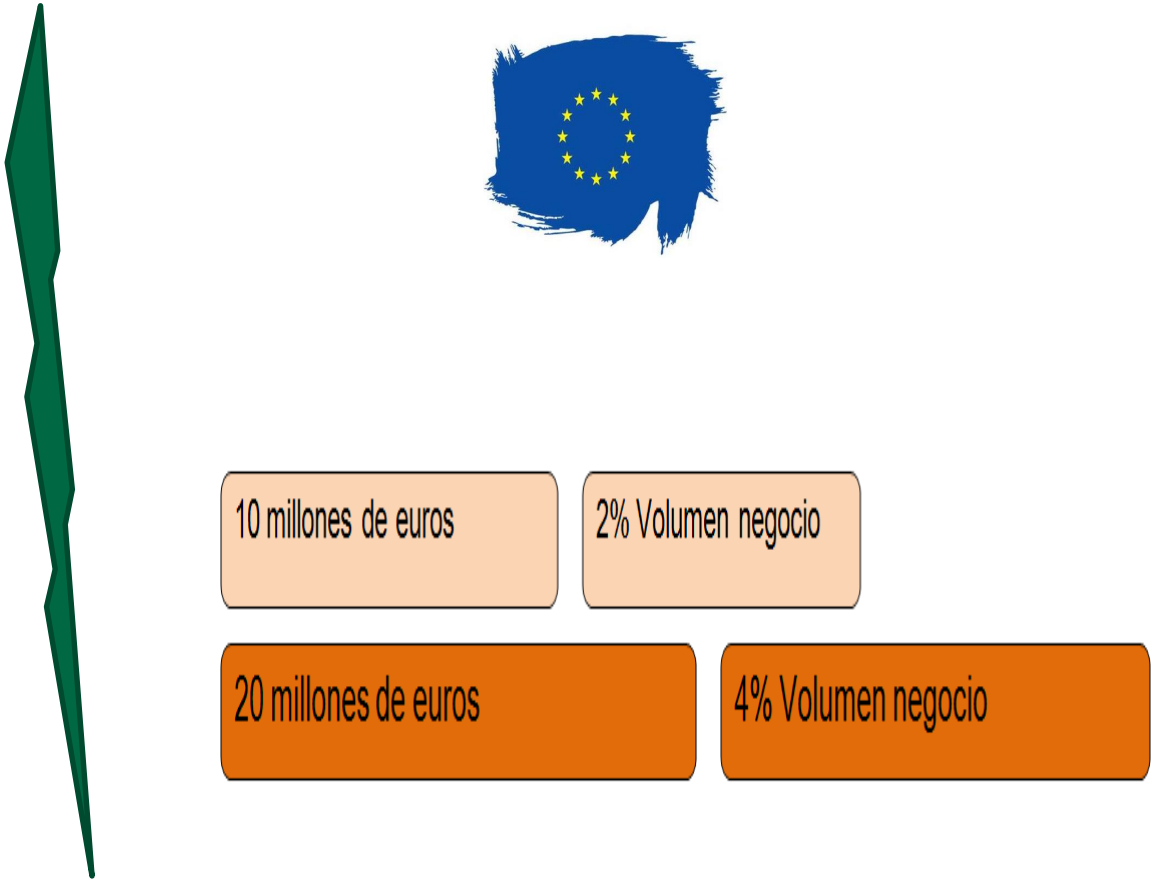
- Controles periódicos
- Auditorías

FASE - MEJORA CONTÍNUA (ACT)

- No Conformidades
- Acciones Correctivas
- Planes de Mejora

ENDURECIMIENTO DE LAS SANCIONES





NLOPD **Tampoco contempla sanciones económicas para el sector público**

EL DPD: ANTECEDENTES

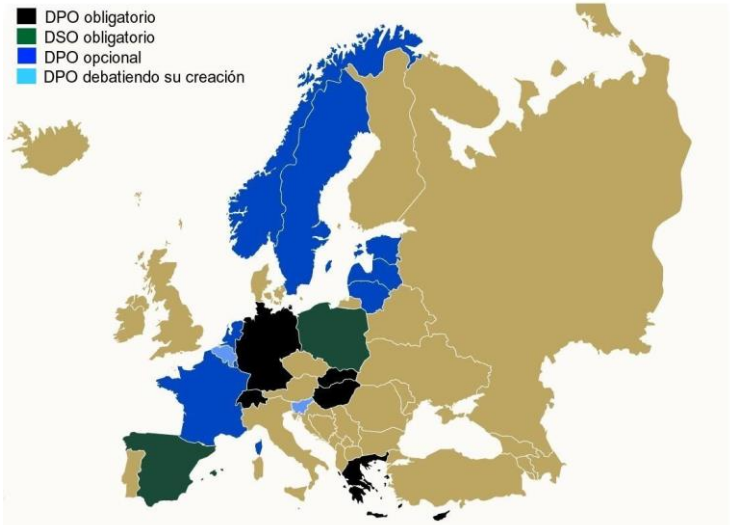
Directiva 95/46 permitía omitir la notificación cuando se dieran ciertas condiciones, entre las que se exigía haber designado DPD.

ANTES LA SITUACIÓN ERA ASIMÉTRICA

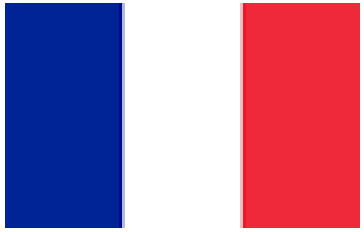
Términos utilizados:

•DPO (Data Protection Officer)

•DSO (Responsable de Seguridad)



•Fuente: http://www.aspectosprofesionales.info/2012/04/el-delegado-de-proteccion-de-datos.html



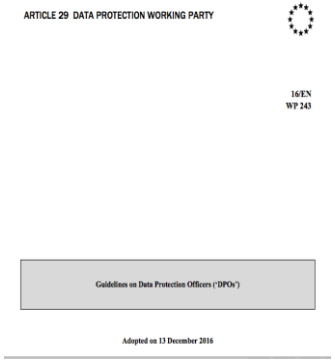
AHORA SUPUESTOS DE OBLIGATORIEDAD DPD

RGPD

*1. Cuando el tratamiento lo lleve a cabo **una autoridad u organismo público,** excepto los tribunales que actúen en ejercicio de su función judicial".*

*2. Cuando las **actividades principales** consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una **observación habitual y sistemática** de interesados a **gran escala".***

*3. Cuando as **actividades principales** consistan en el tratamiento a gran escala **de categorías especiales de datos y de datos relativos a condenas e infracciones penales.***


ARTICLE 29 DATA PROTECTION WORKING PARTY

16/EN
WP 243

Guidelines on Data Protection Officers ('DPOs')

Adopted on 13 December 2016

NLOPD

Supuestos concretos.

CONVENIENCIA

1. Elevadas sanciones previstas
2. Mayor importancia dada al activo datos personales
3. Mayor complejidad

NLOPD *"Los responsables o encargados del tratamiento no incluidos en el párrafo anterior podrán designar un delegado de protección de datos voluntario, que quedará sometido al régimen establecido en este capítulo".*

FUNCIONES DEL DPD

RGPD

1. **Informar y asesorar** al responsable, al encargado y empleados.

2. **Supervisar el cumplimiento incluyendo asignación de responsabilidades, concienciación y formación del personal.**

3. **Asesorar acerca de la evaluación de impacto** y supervisar su aplicación.

4. **Cooperar con la autoridad de control**

5. **Actuar como punto de contacto** en cuestiones relativas al tratamiento de los datos, incluyendo las consultas previas.

Según el **ESQUEMA DE CERTIFICACIÓN DE DPD Y RECOMENDACIONES AEPD para AAPP:**

¿Y la segregación de funciones?

1. Cumplimiento de principios relativos al tratamiento: limitación de finalidad, minimización o exactitud de los datos
2. Identificación de las bases jurídicas de los tratamientos
3. Valoración de compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos
4. Existencia de normativa sectorial que pueda determinar condiciones de tratamiento específicas
5. Diseño e implantación de medidas de inform datos
6. Establecimiento de mecanismos de recep io de derechos por parte de los interesados
7. Valoración de las solicitudes de ejercicio de
8. Contratación de encargados de tratamiento, s jurídicos requeridos
9. Identificación de los instrumentos de TID icas de la organización y de las razones que la
10. Diseño e implantación de políticas de protec
11. Auditoría de protección de datos
12. Establecimiento y gestión de los registros de
13. Análisis de riesgo de los tratamientos realiza
14. Implantación de las medidas de protección d adas a los riesgos y naturaleza de los tratamientos
15. Implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos
16. Establecimiento de procedimientos de gestión de violaciones de seguridad de los datos y de notificación a las autoridades y a los afectados
17. Determinación de la necesidad de realización de evaluaciones de impacto sobre la protección de datos
18. Realización de evaluaciones de impacto sobre la protección de datos
19. Relaciones con las autoridades de supervisión
20. Implantación de programas de formación y sensibilización del personal en materia de protección de datos

NLOPD Gestión de reclamaciones

- Cuando se haya designado un **DPD**

- **GESTIÓN PREVIA A LA RECLAMACIÓN:**

    - El afectado se podrá dirigir al DPD de la entidad contra la que se reclame.
    - El DPD comunicará al afectado la decisión que se hubiera adoptado en el plazo máximo de dos meses a contar desde la recepción de la reclamación.

- Si el afectado presenta **RECLAMACIÓN DIRECTAMENTE ANTE LA AUTORIDAD DE CONTROL:**

    - Las autoridades podrán remitir la reclamación al delegado de protección de datos a fin de que por el mismo se dé respuesta a la misma en el plazo de un mes.

POSIBILIDADES DE CONFIGURACIÓN

INTERNO/EXTERNO

Dependerá del tipo, actividad y tamaño de organización

UNIPERSONAL O COLECTIVO

La organización cual se adapta mejor a sus necesidades.

NLOPD Dice que puede ser una persona física o jurídica

.

POSICIÓN DEL DPD

- **PARTICIPACIÓN del DPD** en todas las cuestiones relativas a la protección de datos personales

- **RECURSOS NECESARIOS**

- **INDEPENDENCIA**

  - No recibirá instrucciones.
  - Depende directamente del más alto nivel jerárquico.

- **DESPIDO O SANCIÓN**

  - **Concepto amplio de sanción**
  - **No podrá ser sancionado o destituido por el hecho de desempeñar sus funciones…. NLOPD:** *salvo que incurriera en dolo o negligencia grave en su ejercicio".*

- **COMPATIBILIDAD CON OTRAS FUNCIONES. ANÁLISIS DE CONFLICTO DE INTERESES.**

CUALIDADES DEL DPD

EXPLÍCITAS (ART. 37 RGPD)

1. Cualidades profesionales
2. Conocimientos especializados del Derecho
3. Práctica en materia de protección de datos
4. Capacidad para ejecutar las tareas contempladas en el art. 39.

Considerando 97:

El nivel de conocimientos especializados necesario se debe determinar, en particular, ***en función de las operaciones de tratamiento de datos*** *que se lleven a cabo y de la protección exigida para los datos personales tratados por el responsable o el encargado.*

IMPLÍCITAS:

1. CONOCIMIENTO SECTORIAL

2. CAPACIDAD DE COMUNICACIÓN

3. CONOCIMIENTO DE IDIOMAS

4. MUY IMPORTANTE: CONOCIMIENTO DE GESTIÓN DE RIESGOS

+ OTRAS QUE RECOMIENDA EL GTA29

Ej. DPO sector público Derecho administrativo

¿CÓMO ACREDITAR LOS CONOCIMIENTOS?. FORMACIÓN/CERTIFICACIÓN

- **NLOPD** Puede acreditar la capacitación por diferentes medios, incluída le certificación
- No se exige disponer de una certificación para ser DPD.
- No obstante, puede ser una buena práctica y es altamente recomendable.
- La AEPD como Propietaria del Esquema y ENAC como entidad de acreditación han constituido el Esquema de Certificación de DPD.


La AEPD presenta junto a ENAC su Esquema de certificación de Delegados de Protección de Datos

- Las certificaciones serán otorgadas por entidades de certificación acreditados por ENAC, siguiendo criterios de certificación elaborados por la AEPD en colaboración con los sectores afectados.

PRERREQUISITOS

- Balancea formación y experiencia

- **EXPERIENCIA/FORMACIÓN MÍNIMA**

EXPERIENCIA MÍNIMA	FORMACIÓN MÍNIMA
5 años	No exigida
3 años	60 horas
2 años	100 horas
Sin experiencia	180 horas

NOTAS:

1. Respecto a la formación:
   a) Se refiere a que sea recibida y/o impartida
   b) El temario también está definido en el esquema.
2. En caso de no alcanzar la experiencia se podrá convalidar por méritos adicionales.

3. En cualquier caso, en todas las modalidades se requiere la superación de un examen.

CREO QUE TODA ORGANIZACIÓN DEBIERA PLANTEARSE ESTAS PREGUNTAS…

¿Mi organización tiene una hoja de ruta para adecuarse al RGPD?

Y descendiendo al **DPD:**

1. ¿Mi organización debe de tener o le interesa tener un DPD?
2. ¿Sé quién o quiénes deben de asumir este rol?
3. ¿Cómo se conjugará con otros roles y responsabilidades existentes?
4. ¿Sería mejor interno o externo? ¿individual o colectivo?
5. ¿Cuáles son las tareas que deberá de acometer?
6. ¿Tiene la capacitación para ejecutarlas?

QAEC

Insight exclusivo AEC

Descubre las claves de la nueva figura del

Delegado de Protección de Datos

DPD / DPO

16 de noviembre de 2017