JORNADA **APLICANDO LA NUEVA NORMATIVA SOBRE PROTECCIÓN DE DATOS**

Junta de Castilla y León

VALLADOLID, 17 DE OCTUBRE 2018

eclap

Julián Prieto Hergueta

Agencia Española de Protección de Datos

MARCO JURÍDICO

- CONVENCIÓN 108 de 1981 y Protocolo adicional
- REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS 2016/679
- DECRETO-LEY 5/2018,
- OTRAS NORMAS (soft law):
  - Decisiones CE: Adecuación, Cláusulas contractuales tipo
  - Directrices OCDE (1980)
  - Directrices NNUU (1990)
  - Estándares internacionales (2009)
  - Sentencia Lindqvist
  - Sentencia Schrems
  - Relevancia documentos del Grupo del Artículo 29/CEPD
- PRLOPD y DG
- DIRECTIVA 2016/680 para tratamiento de datos por autoridades competentes en prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales
- Normas sectoriales

NORMATIVA DE PROTECCIÓN DE DATOS

REAL DECRETO LEY 5/2018, de 27 de julio, sobre medidas urgentes para la adaptación al Derecho español a la normativa de la Unión Europea en materia de protección de datos:

- Capítulo I: Inspección en materia de protección de datos
- Capítulo II: Régimen sancionador
- Capítulo III: Procedimientos en casos de infracción de la normativa de protección de datos
- Disposiciones:
  - Representación en el CEPD (adicional)
  - Participación Publicación resoluciones AEPD (adicional)
  - Régimen transitorio procedimientos
  - Contratos con encargados del tratamiento (transitorio)
  - Mantenimiento art.46 LOPD para las AAPP

PROYECTO LOPD

PROYECTO DE LEY ORGÁNICA DE PROTECCIÓN DE DATOS Y PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES (en tramitación)

- Incorporar al Derecho nacional previsiones interpretación RGPD, cuando sea necesario. Complemento del RGPD
- Regulación datos personas fallecidas
- Se fija la edad del menor
- Regula posibles tratamiento concretos, entre ellos, el de los Sistemas de denuncias internas, videovigilancia, solvencia,…
- Relación de entidades que requieren DPD y su configuración como figura para resolver conflictos en protección de datos
- El Régimen de la AEPD
- Procedimiento sancionador (inicio del procedimiento de ventanilla única) y sanciones (sustituirá a las disposiciones del DL)
- Derechos digitales

ÁMBITO DE APLICACIÓN MATERIAL

Artículo 2

"1. El presente Reglamento se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero".

Necesidad de superar la idea de fichero como eje de la normativa de protección de datos, que descansa en el concepto de tratamiento. La noción de fichero es meramente residual para el caso de tratamiento no automatizado

FICHERO: ***todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica***

EXCLUSIONES

- Actividades no comprendidas en el ámbito de aplicación del Derecho de la UE (seguridad nacional)
- Tratamiento por los Estados miembros en materia de política exterior y de seguridad común
- Tratamiento efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas
- Tratamientos sometidos a efectos de prevención, investigación, detección o enjuiciamiento de infracciones penales, o la ejecución de sanciones penales, incluida la protección frente a a las amenazas contra la seguridad pública por las autoridades competentes (Directiva 2016/680)
- Tratamiento por las instituciones, órganos y organismos de la Unión (Reglamento (CE) 45/2001 que deberá adaptarse)
- Los datos de las personas fallecidas. No se aplica el Reglamento pero los Estados miembros son competentes para establecer normas relativas al tratamiento de los datos personales de éstas (lo recoge el PLOPD)

Ámbito territorial de aplicación

Artículo 3

"1. El presente Reglamento se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado del tratamiento en la Unión.

2. El presente Reglamento se aplica al tratamiento de datos personales de interesados que residan (que estén o se encuentren) en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con:

a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere un pago

b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión"

RESPONSABILIDAD PROACTIVA

El Reglamento prevé que los responsables aplicarán las **medidas técnicas y organizativas apropiadas para garantizar y estar en condiciones de demostrar que el tratamiento de datos personales se lleva a cabo de conformidad con el presente Reglamento**. Tales medidas se revisarán y actualizarán cuando sea necesario

RESPONSABILIDAD PROACTIVA

Tipos de medidas

- Mantener "Registro de actividades de tratamiento"
- Medidas de Protección de Datos desde el Diseño
- Medidas de Protección de Datos por Defecto
- Aplicar medidas de seguridad adecuadas
- Llevar a cabo Evaluaciones de Impacto
- Autorización previa o consultas previas con APD
- Designación Delegado Protección de Datos (DPD)
- Notificación de Quiebras de Seguridad
- Códigos de conducta y esquemas de certificación
- Contratos encargados del tratamiento

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

El RGPD suprime la obligación de notificar los tratamientos al registro general de protección de datos

En su lugar, el RGPD impone al responsable y al encargado la obligación de mantener un registro de actividades de tratamiento

Contenido del Registro (RESPONSABLES):

- El responsable, su representante y el DPD, en su caso
- Finalidad para la que se recogen y tratan los datos
- Descripción interesados, datos, destinatarios y transferencias internacionales
- Plazo conservación, cuando sea posible
- Descripción general medidas seguridad, cuando sea posible

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

Contenido del Registro (ENCARGADOS):

- Datos contacto encargado y de cada responsable por cuenta del cuál actúe. Su representante y el DPD, en su caso
- Categorías de tratamientos efectuados por cada responsable
- Transferencias internacionales de datos, en su caso
- Descripción general medidas seguridad, cuando sea posible

El Registro constará por escrito, inclusive en formato electrónico

A disposición de la Agencia

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

Organización del Registro:

- Partir de los ficheros notificados al RGPD, Por ejemplo, en torno a conjuntos estructurados de datos (ficheros): finalidades, categorías de interesados,…

https://sedeagpd.gob.es/sede-electronica-web/vistas/formCopiaContenido/copiaContenido.jsf

- PLOPD, inclusión de la base jurídica
- PLOPD, inventarios de los tratamientos sector público accesibles por medios electrónicos (art. 31.2)

Excepciones: Menos de 250 empleados salvo: Riesgo derechos y libertades, no sea ocasional, no incluya categorías especiales de datos, ni de condenas e infracciones penales

Responsabilidad

Campo	Descripción
Responsable del tratamiento	Nombre y datos de contacto del responsable y, en su caso, del corresponsable o del representante del responsable
Delegado de Protección de Datos	Nombre y datos de contacto del Delegado de Protección de Datos

Descripción de la actividad de tratamiento y de los datos tratados

Campo	Descripción
Actividad de Tratamiento	Conjunto de operaciones, procesos o procedimientos, automatizados o manuales, que conlleve la recogida, consulta, grabación, modificación, cesión o destrucción de datos de carácter personal
Finalidad	Descripción de los fines explícitos y la base jurídica en virtud de los cuales el Responsable del tratamiento procede a la realización de las actividades de tratamiento sobre datos personales
Interesados	Categorías de personas físicas identificadas o identificables a quien corresponden los datos personales que son tratados: ■ Clientes ■ Empleados ■ Proveedores ■ Etc.
Categorías de datos personales	Detalle de los datos objeto del tratamiento en función de su clasificación: ■ Datos identificativos (nombre, DNI, dirección, ...) ■ Datos financieros (cuenta bancaria, solvencia, ...) ■ Datos profesionales (profesión, experiencia, ...) ■ Datos de salud (enfermedades, alergias, ...) ■ Datos ideológicos y políticos ■ Datos de menores (herencia, seguros, ...) ■ Otros tipos de datos: especificar qué datos.

Transferencias y cesiones

Campo	Descripción
Cesiones	Categorías de destinatarios a quienes se comunicaron o se comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales.
Transferencias de datos internacionales	Identificación de transferencias internacionales de los datos. Se debe identificar a dicho tercer país u organización internacional junto a la base jurídica que la hace posible en ausencia de una decisión de adecuación o de garantía adecuadas: ■ Consentimiento explícito del interesado a la transferencia ■ Transferencia necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento ■ Transferencia necesaria para la celebración o ejecución de un contrato, en interés del interesado, entre el responsable del tratamiento y otra persona física o jurídica ■ Transferencia necesaria por razones importantes de interés público ■ Transferencia necesaria para la formulación, el ejercicio o la defensa de reclamaciones ■ Transferencia necesaria para proteger los intereses vitales del interesado o de otras personas Si fuese de aplicación, medidas y garantías adecuadas adoptadas.
Periodo de conservación	Indicador de los plazos de conservación de la información establecidos en función del tratamiento, la finalidad, la categoría del dato y las leyes establecidas.

Medidas de seguridad

Campo	Descripción
Medidas de seguridad	Descripción general de las medidas técnicas y organizativas de seguridad

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

ACTIVIDAD AEPD "Gestión presupuestaria y económica"

a) Base jurídica

RGPD: 6.1.c) Tratamiento necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento.

Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.

Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba la Ley del Estatuto Básico del Empleado Público.

Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público.

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

Ley 47/2003, de 26 de noviembre, General Presupuestaria.

Ley 58/2003, de 17 de diciembre, General Tributaria.

Plan General de Contabilidad Pública en relación con la Disposición Final Primera de la Ley 16/2007, de 4 de julio.

Real Decreto 462/2002, de 24 de mayo, sobre indemnizaciones por razón de servicio.

Ley 38/2003, de 17 de noviembre, General de Subvenciones.

Ley 40/2005, de 1 de octubre, de Régimen Jurídico del Sector Público.

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

b) Fines del tratamiento

Tramitación de expedientes de gasto e ingresos derivados de la ejecución del presupuesto de la AEPD y de su actividad sancionadora.

c) Colectivo

Personal, funcionario y laboral, de la AEPD, proveedores, beneficiarios de subvenciones, sancionados, licitadores.

c) Categorías de Datos

Nombre y apellidos, DNI/NIF/Documento identificativo, dirección, firma y teléfono.

Datos de detalle de empleo: puesto de trabajo.

Datos económico financieros y de seguros: Datos bancarios.

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

d) Categoría destinatarios

Del personal de la AEPD: Entidades financieras. Instituto Nacional de la Seguridad Social y mutualidades de funcionarios. Agencia Estatal de Administración Tributaria. Intervención General de la Administración del Estado. Tribunal de Cuentas.

Para los licitadores y los firmantes de contratos con la AEPD: Plataforma de contratación del Estado. Registro público de contratos.

e) Transferencias Internacionales

No están previstas transferencias internacionales de los datos.

f) Plazo supresión

Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad y del tratamiento de los datos, conforme a la Ley 58/2003, de 17 de diciembre, General Tributaria, además de los periodos establecidos en la normativa de archivos y documentación.

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

g) Medidas de seguridad

Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica y que se encuentran descritas en los documentos que conforman la Política de protección de datos y seguridad de la información de la AEPD.

h) Entidad responsable

Agencia Española de Protección de Datos

https://www.aepd.es/agencia/transparencia/registro-actividades-tratamiento/index.html

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

Tratamientos típicos de las Administraciones locales:

- Padrón municipal de habitantes
- Gestión de tributos
- Gestión económica
- Recursos humanos
- Policía Local
- Sanciones
- Obras y licencias
- Biblioteca
- Servicios sociales
- Subvenciones y ayudas
- Videovigilancia y control de acceso

Categorías de datos objeto de tratamiento por las Administraciones locales:

- Identificativos: nombre y apellidos, dirección, teléfono, imagen DNI/NIE
- Tributarios: para la gestión de los tributos municipales
- Académicos y profesionales
- Financieros: bancarios
- Derivados del ejercicio de la potestad sancionadora (infracciones, sanciones)
- Categorías especiales de datos: salud, afiliación sindical
- vida sexual

Protección de Datos desde el diseño

- **Medidas técnicas y organizativas adecuadas** (p.ej. seudonimización, minimización) para aplicar principios de PD de forma eficaz y proteger los derechos
- **En el momento de determinar los medios para el tratamiento y en el momento del tratamiento** (integrar necesarias garantías)
- Teniendo en cuenta
  - Naturaleza, ámbito, contexto y fines del tratamiento
  - Riesgos de diversa probabilidad y gravedad (no sólo alto riesgo)
  - Estado de la técnica y coste

PRIVACIDAD por DEFECTO

Protección de Datos por defecto

- Medidas técnicas y organizativas apropiadas
- Tratamiento **por defecto sólo de datos personales necesarios para cada fin específico**
  - Cantidad de datos recopilados
  - Extensión del tratamiento
  - Periodo de almacenamiento
  - Accesibilidad
  - En particular, evitar la accesibilidad a un número indeterminado sin intervención de alguien

ANÁLISIS DE RIESGOS

Necesidad de llevar a cabo un análisis de riegos para los derechos y libertades de los ciudadanos de todos los tratamientos de datos desarrollados por el responsable

Necesario para determinar las medidas técnicas y organizativas que habrán de imponerse sobre el tratamiento

- **FACILITA**
- **GUÍA DE ANÁLISIS DE RIESGOS**
- Actualmente en el ámbito público existen metodologías y herramientas de análisis de riesgos (MAGERIT, PILAR) para determinar las medidas de seguridad de la información

ANÁLISIS DE RIESGOS

SUPUESTOS DE RIESGO (C 75)

- Posibles situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados
- Posible privación de derechos y libertades o del control sobre los datos
- Tratamiento de categorías especiales de datos (genéticos, salud, visa sexual,…)
- Evaluación de aspectos personales de los afectados para creación de perfiles
- Afectados en situación de especial vulnerabilidad (menores)
- Tratamiento gran cantidad de datos personales que afecten a un gran número de interesados

MEDIDAS DE SEGURIDAD

- Procederán del resultado del análisis de riesgos
- Responsables y encargados deben aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, teniendo en cuenta
  - Estado de la técnica y costes de aplicación
  - Naturaleza, alcance, contexto y fines del tratamiento
  - Riesgos para los derechos y libertades de las personas
- El Reglamento no establece listado estructurado de medidas, aunque establece algunas prevenciones, como la seudonimización o el cifrado
- La adhesión a un código de conducta o a un mecanismo de certificación podrá servir de elemento para demostrar cumplimiento

SEUDONIMIZACIÓN: tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable

EVALUACIONES DE IMPACTO

Cuando el tratamiento por su naturaleza, alcance, contexto o fines entraña un alto riesgo para los derechos y libertades de las personas físicas. No es un análisis de riesgos, sino una evaluación más detallada y pormenorizada derivada del resultado del análisis previo:

- Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado e implique la adopción de decisiones
- Tratamiento a gran escala de las categorías especiales de datos
- Observación sistemática a gran escala de una zona de acceso público

Además las autoridades de protección de datos publicarán listas de tratamientos que la requieran y de los que no la requieran

- GUÍA DE EVALUACIÓN DE IMPACTO
- No será necesario realizar la EIPD cuando el tratamiento se base en una Ley que la incorpore como parte de la evaluación general de impacto

Si no es posible la adopción de medidas para mitigar el riesgo deberá recabarse la opinión de la autoridad de protección de datos

EVALUACIONES DE IMPACTO

GRAN ESCALA

- Aplicable también para los Delegados de Protección de datos
- No hay cifra exacta
- Directrices Grupo del 29 (WP 243) factores como:
  - Núm. Afectados: cifra concreta o proporción de población correspondiente
  - Volumen, variedad de datos o elementos tratados
  - Duración o permanecía
  - Alcance geográfico
- RGPD no sería gran escala los datos de salud de 1 solo médico o las categorías especiales de 1 solo abogado:
  - Zonas grises
  - No necesariamente se tiene que aplicar igual para los DPD

CONSULTA APD

- Consulta a APD cuando una EIPD muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para mitigarlo *"y el responsable del tratamiento considera que el riesgo no puede mitigarse por medios razonables en cuanto a tecnología disponible y costes de aplicación"*
- APD podrá →
  - Asesorar por escrito al responsable y, en su caso, al encargado
  - Utilizar cualquiera de sus poderes, incluido prohibir el tratamiento
- Obligación de consulta en elaboración de toda propuesta de medida legislativa o de una medida reglamentaria que la aplique
- El derecho nacional podrá establecer consulta y petición de autorización en tratamientos derivados del ejercicio de una misión realizada en interés público

DELEGADO DE PROTECCIÓN DE DATOS

¿QUIÉN ES EL DELEGADO DE PROTECCIÓN DE DATOS?

- **RGPD (Cdo. 97)**
  - **A fin de garantizar el cumplimiento del Reglamento, el responsable o encargado deberá contar con la ayuda de una persona con conocimientos especializados del derecho y la práctica de protección de datos is es una autoridad pública**

DELEGADO DE PROTECCIÓN DE DATOS

El RGPD requiere la designación de un **DPD** en tres casos específicos:

- **CUANDO EL TRATAMIENTO SE REALICE POR UNA AUTORIDAD U ORGANISMO PÚBLICO (INDEPENDIENTEMENTE DE LOS DATOS QUE SE ESTÉN PROCESANDO);**
- Cuando las actividades principales del responsable del tratamiento o del encargado consisten en operaciones de tratamiento que exigen un control periódico y sistemático de los datos a gran escala;
- Cuando las actividades principales del responsable del tratamiento o del encargado consisten en tratar a gran escala categorías especiales de datos o datos personales relativos a condenas y delitos penales.

Por tanto, el RGPD hace obligatoria la figura del DPD en las autoridades y organismos públicos. Podrá designarse un único DPD para varias autoridades u organismos dependiendo de tamaño y características

DELEGADO DE PROTECCIÓN DE DATOS

PLOPD INCLUYE SUPUESTOS QUE RESPONDEN A LOS REQUISITOS RGPD, entre otros:

- Colegios profesionales y sus consejos generales
- Centros educativos y universidades
- Centros sanitarios
- Prestadores de servicios de información que elaboren perfiles de usuarios a gran escala
- Entidades de ordenación, supervisión y solvencia de entidades de crédito
- Aseguradoras y reaseguradoras
- Responsables de ficheros comunes de solvencia patrimonial
- Operadores del juego
- Federaciones deportivas que traten datos de menores
- …

DELEGADO DE PROTECCIÓN DE DATOS

Funciones

- **Informar y asesorar** a responsable y encargado, documentando esa actividad
- **Supervisar** la puesta en práctica de las **políticas de protección de datos**, incluidas la formación y la auditoría
- **Supervisar** la aplicación del Reglamento en lo relativo a **PbD**, **PbDef y derechos de los interesados**
- Asegurar la existencia y mantenimiento de documentación obligatoria
- **Supervisar gestión de quiebras de seguridad**

DELEGADO DE PROTECCIÓN DE DATOS

- **Supervisar** la realización de **Evaluaciones de Impacto y la solicitud de autorizaciones o consultas** que se requieran
- Supervisar respuestas a requerimientos de APD
- Cooperar con la APD en el marco de sus tareas
- Actuar como **punto de contacto para la APD y los interesados**
- Comunicación **de su identidad al público**
- Derecho **de acceso por los interesados**
- Información **directa a la dirección**

DELEGADO DE PROTECCIÓN DE DATOS

El RGPD exige que el DPD «se designe sobre las base de cualidades profesionales y, en particular, conocimientos especializados sobre la legislación y las prácticas en materia de protección de datos y sobre la capacidad para cumplir las tareas a que se refiere el artículo 39»

Los DPD no son personalmente responsables por el incumplimiento del RGPD. El RGPD y el Decreto Ley dejan claro que es el responsable del tratamiento o del encargado quien debe garantizar y demostrar que el tratamiento se realiza de conformidad con el presente Reglamento. El cumplimiento de la protección de datos es responsabilidad del responsable o del encargado

DELEGADO DE PROTECCIÓN DE DATOS

Habilidades y experiencia :

- Experiencia en las leyes y prácticas nacionales y europeas en materia de protección de datos, incluida una comprensión en profundidad del RGPD
- Comprensión de las operaciones de tratamiento realizadas
- Comprensión de las tecnologías de la información y la seguridad de los datos
- Conocimiento del sector empresarial y de la organización
- Capacidad para promover una cultura de protección de datos
- No se prevé cómo acreditar cualidades profesionales
- Esquema de certificación de ENAC

RECURSOS A DISPOSICIÓN DE LOS DPD

Dependiendo de la naturaleza de las operaciones de tratamiento y las actividades y tamaño de la organización:

- **Apoyo activo de la función del DPD por parte de la alta dirección**
- **Disponibilidad de tiempo para cumplir sus obligaciones**
- **Apoyo adecuado en términos de recursos humanos y materiales**
- **Comunicación oficial de la designación del DPD a la AEPD y a todo el personal**
- **Acceso a otros servicios dentro de la organización para que los DPD puedan recibir apoyo esencial, aportaciones o información de esos otros servicios**
- **Acceso a los tratamientos de datos**
- **Formación continua**

DELEGADO DE PROTECCIÓN DE DATOS

EJERCE SUS FUNCIONES DE MANERA INDEPENDIENTE

- Ninguna instrucción de los responsables o encargados sobre el ejercicio de las tareas del **DPD**
- Ningún despido o sanción al delegado por el desempeño de sus tareas, salvo dolo o negligencia grave
- Ausencia de conflicto de intereses con otras posibles tareas y deberes
  - El DPD no puede ocupar un puesto dentro de la organización que lo conduzca a determinar los propósitos y los medios del tratamiento de los datos personales. Debido a la estructura organizativa específica en cada organización, esto debe ser considerado caso por caso.
  - Como regla general, las posiciones conflictivas pueden incluir posiciones de alta dirección, jefe de Recursos Humanos o jefe de departamentos de TI, pero también otros roles más bajos en la estructura organizativa si tales posiciones o roles conducen a la determinación de propósitos y medios de tratamiento

BRECHAS DE SEGURIDAD

El RGPD impone la obligación de notificar las violaciones de seguridad

- **A las autoridades de protección de datos en un máximo de 72 horas desde que se tenga constancia de ellas, a menos que sea improbable que constituyan un riesgo para los derechos y libertades de las personas físicas**
  - **Deberán documentarse la violación, los hechos producidos, sus efectos y las medidas correctoras**
    - **Registro de incidentes de seguridad**
  - **Deberá facilitarse gradualmente cualquier información adicional**
- **Al interesado**
  - **Si es probable que se genere una situación de alto riesgo para sus derechos y libertades**
  - **Por iniciativa propia o por exigencia de la autoridad de protección de datos**

GUÍA SOBRE BRECHAS DE SEGURIDAD

CÓDIGOS DE CONDUCTA Y CERTIFICACIONES

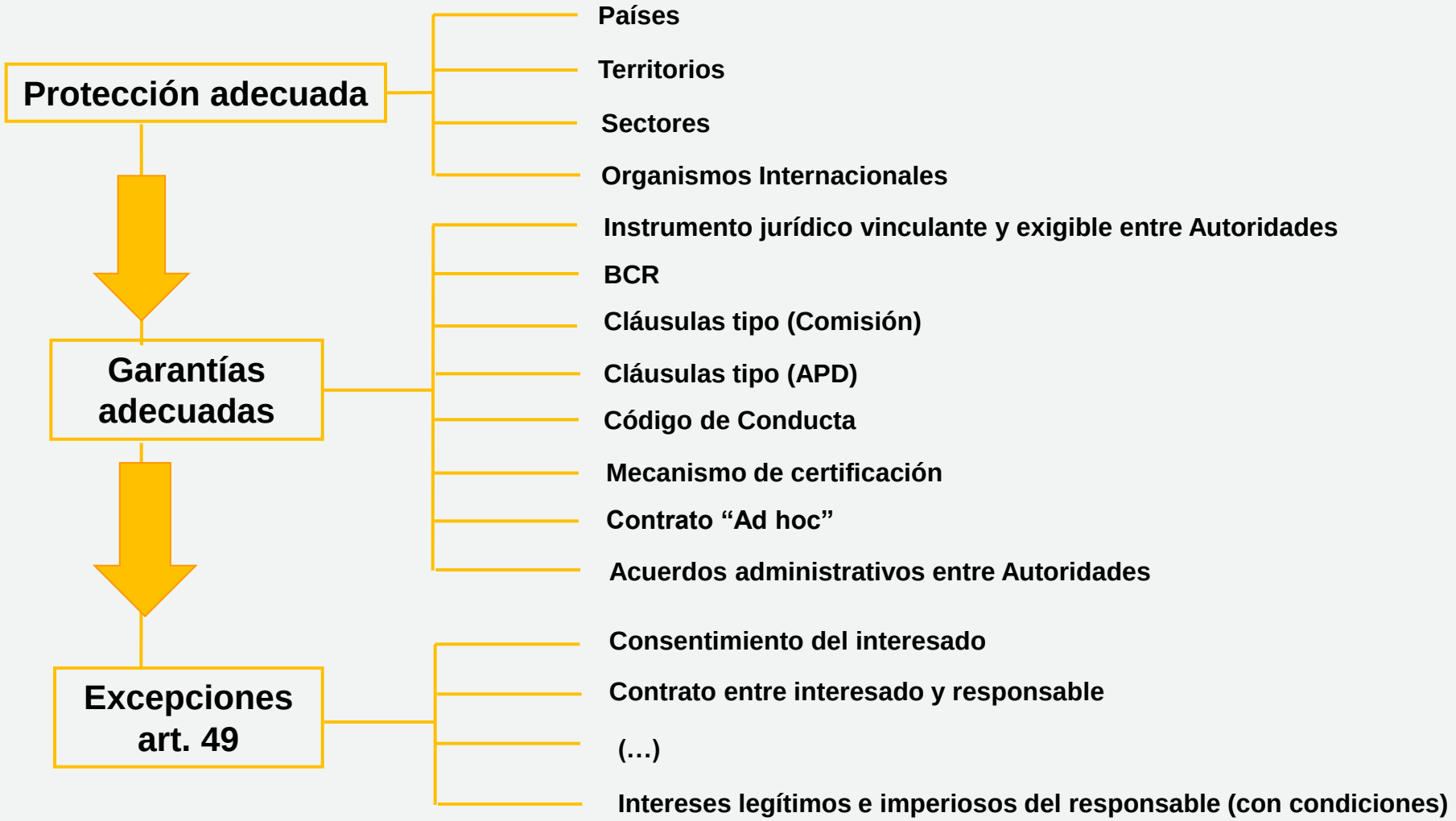
- ***Códigos*** → **"facilitar la aplicación efectiva, del RGPD teniendo en cuenta las características específicas del tratamiento llevado a cabo en determinados sectores y las necesidades específicas de las PYMES"**
- ***Certificaciones*** → ***"permitir a los interesados evaluar con mayor rapidez el nivel de protección de datos de los productos y servicios correspondientes"***
- ***Demostrar el cumplimiento de lo dispuesto en el RGPD***

TRANSFERENCIAS INTERNACIONES DE DATOS

TID sólo posibles si:

- Se cumplen disposiciones de RGPD y
- Hay nivel de protección adecuado, **o**
- Se ofrecen garantías suficientes, **o**
- Concurre una causa excepcional

TRANSFERENCIAS INTERNACIONALES DE DATOS



TRANSFERENCIAS INTERNACIONALES DE DATOS

Movimientos internacionales de datos
Régimen de autorizaciones

EEE No transferencia internacional

Resto países. Transferencias internacionales

Sin autorización APD

- Nivel Adecuado
- Instrumento Jurídico Vinculante
- BCR
- CT Comisión
- CT APD y Comisión
- Códigos de Conducta
- Certificaciones
- Excepciones

Autorización APD

- Contratos "Ad Hoc"
- Acuerdo administrativos entre autoridades (MoU)

Información a la APD

- Interés legítimo imperioso del responsable

TRANSFERENCIAS INTERNACIONALES DE DATOS

- **Con autorización previa de APD sólo →**
  - **Cláusulas "ad hoc" autorizadas por APD nacional**
  - **Disposiciones en acuerdos administrativos entre autoridades u organismos públicos (MoU)**
- **Todos estos instrumentos han de contener derechos exigibles y acciones legales efectivas para los interesados**
- **Decisiones de APD tomadas sobre Directiva 95/46 siguen siendo válidas hasta que las APD las modifiquen, sustituyan o deroguen**

TRANSFERENCIAS INTERNACIONALES DE DATOS

DESTINOS CON NIVEL DE PROTECCIÓN ADECUADA

DECISIONES DE ADECUACIÓN ADOPTADAS POR LA COMISIÓN EUROPEA (Directiva 95/46)

Suiza, Argentina, Guernsey, Man, Jersey, Islas Feroe, Andorra, Israel, Uruguay y Nueva Zelanda

Canadá (ley canadiense Personal Information and Electronic Documents Act)

USA (PRIVACY SHIELD)

ENCARGADOS DE TRATAMIENTO

- Obligación general de diligencia en selección de encargado
- Regulación más detallada que en Directiva y asimilada a la española
  - En el contenido del instrumento que exterioriza la relación jurídica
  - En las obligaciones del encargado
  - En el régimen de posible subcontratación
- Algunas peculiaridades:
  - Previsión de que el responsable "realice auditorías y contribuya a ellas, incluidas las inspecciones dirigidas por el responsable o por otro auditor autorizado por dicho responsable"
  - Fin de la prestación implica borrado o devolución de datos, sin incluir transferencia a otro encargado
    - Posible vinculación al derecho a la portabilidad
  - Obligación de informar al responsable "si, en su opinión, una instrucción infringe el presente Reglamento o las disposiciones nacionales o de la Unión en materia de protección de datos"
  - Posibilidad de "contratos modelo"

ENCARGADOS DEL TRATAMIENTO

Decreto Ley 5/2018 (Disposición transitoria segunda)

Los contratos de encargado del tratamiento suscritos con anterioridad al 25 de mayo de 2018 al amparo de lo dispuesto en el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal mantendrán su vigencia hasta la fecha de vencimiento señalada en los mismos y, en caso de haberse pactado de forma indefinida, hasta el 25 de mayo de 2022.

Durante dicho plazo cualquier de las partes podrá instar a la otra la modificación del contrato a fin de adecuarlo al RGPD.

ADAPTACIÓN AL RGPD – Administraciones Públicas

1. **DESIGNAR UN DELEGADO** de Protección de Datos, si procede. (Ver art.37 *RGPD* y art. 34 *PLOPD*)

2. **ELABORAR EL** Registro de Actividades de tratamiento, prestando atención especialmente a los tratamientos que incluyan categorías especiales de datos o datos de menores, teniendo en cuenta su finalidad y la base jurídica *(servicio de solicitud de copia de la inscripción como ayuda)*

3. **ANALIZAR** las **BASES JURÍDICAS** de los **TRATAMIENTOS**

4. **EFECTUAR UN ANÁLISIS DE RIESGOS.** Sobre los resultados de ese análisis, identificar e implantar las **MEDIDAS TÉCNICAS Y ORGANIZATIVAS** necesarias para hacer frente a los riesgos detectados sobre los derechos y libertades de los ciudadanos

5. **VERIFICAR LAS MEDIDAS DE SEGURIDAD** tras el resultado del análisis de riesgos. Ello incluye verificar la aplicación de medidas de seguridad adecuadas, así como **ESTABLECER PROTOCOLOS PARA GESTIONAR Y, EN SU CASO, NOTIFICAR** quiebras de seguridad

6. **SI EL TRATAMIENTO ES DE ALTO RIESGO, DETALLAR E IMPLANTAR UN PROCEDIMIENTO** para realizar, una evaluación de impacto de la privacidad y, si fuera necesario, consultar previamente a la autoridad de control (art. 35 y 36, *RGPD*)

HOJA DE RUTA

ADECUAR LOS FORMULARIOS para adaptar el derecho de información a los requisitos del RGPD

ADAPTAR LOS PROCEDIMIENTOS para atender los derechos de los ciudadanos, habilitando medios electrónicos

ESTABLECER Y REVISAR LOS PROCEDIMIENTOS para acreditar el consentimiento y garantizar la posibilidad de revocarlo

VALORAR SI LOS ENCARGADOS DE TRATAMIENTO OFRECEN GARANTÍAS de cumplimiento del RGPD y adaptar los contratos elaborados previamente

CONFECCIONAR E IMPLANTAR POLÍTICAS DE PROTECCIÓN DE DATOS que contemplen los requisitos del *RGPD* (art. 24, 25, 30) y poder acreditar su cumplimiento

ELABORAR Y LLEVAR A CABO UN PLAN DE FORMACIÓN Y CONCIENCIACIÓN para los empleados

¡MUCHAS GRACIAS!