REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS Y LEY DE PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES

Julián Prieto Hergueta

Agencia Española de Protección de Datos

Marzo 2019

En la vida cotidiana es habitual que la persona vaya dejando una estela de datos de carácter personal en sus relaciones, de forma presencial o a distancia, con empresas, profesionales, asociaciones, fundaciones … y con la Administración Pública.

Una persona facilita datos personales cuando abre una cuenta en el banco, cuando se matricula en un curso, cuando reserva un hotel o un vuelo, cuando busca trabajo, cuando presenta una instancia en la Administración Pública, cuando solicita un abono de transporte … siendo múltiples los rastros de datos que se dejan a menudo en todas estas gestiones.

RECONOCIMIENTO COMO DERECHO FUNDAMENTAL

UNIÓN EUROPEA

Carta de Derechos Fundamentales de la Unión Europea: art. 8.1
Artículo16.1 del Tratado de Funcionamiento de la UE (TFUE)

ESPAÑA

Constitución 78: art. 18.4
Tribunal Constitucional, sentencias 290/2000 y 292/2000: Reconocimiento de un derecho fundamental autónomo del derecho a la intimidad personal y familiar

EL DERECHO A LA PROTECCIÓN DE DATOS

DERECHO AUTÓNOMO

- ✓ **Poder de disposición y control sobre los propios datos personales**
- ✓ **Facultad de decidir sobre**
  - **Qué datos se pueden recabar**
  - **Qué datos ceder a un tercero**
- ✓ **Facultad de conocer**
  - **Quién posee esos datos personales**
  - **Para qué los posee**
  - **A quién se van a ceder**
- ✓ **Facultad de oponerse a su posesión o uso**
  - **Solicitando su rectificación o supresión**
  - **Revocando el consentimiento para su uso**

EL DERECHO A LA PROTECCIÓN DE DATOS

DIFERENCIAS CON EL DERECHO A LA INTIMIDAD

- **STC 254/1993**: el artículo 18.4 de la Constitución consagra un **derecho fundamental autónomo y diferente** del derecho a la intimidad: "*una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de las personas: el uso ilegítimo del tratamiento mecanizado de datos*".

- **Distinta función**:
  - Protección de datos: garantizar control de los datos personales.
  - Intimidad: proteger frente a invasiones en la vida privada o familiar.
- **Distinto objeto**:
  - Protección de datos: cualquier tipo de datos.
  - Intimidad: datos íntimos.
- **Distinto contenido**:
  - Protección de datos: obligaciones e instrumentos para hacerlo efectivo: derechos frente al responsable.
  - Intimidad: no.
- **Derecho instrumental.**

MARCO JURÍDICO

CONVENCIÓN 108 de 1981 y Protocolo adicional del Consejo de Europa
REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS 2016/679
LEY ORGÁNICA 3/2018, DE PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES (LOPDPGDD)
OTRAS NORMAS (soft law):

1. **Decisiones Comisión Europea: Adecuación, cláusulas contractuales tipo**
2. **Circulares AEPD (1/2019 sobre tratamiento de datos por partidos políticos en periodo electoral)**
3. **Recomendaciones, directrices… del Comité Europeo de Protección de datos (CEPD)**
4. **Sentencias TJUE: (Lindqvist, Schrems)**
5. **Estándares internacionales (2009)**
6. **Directrices OCDE (1980)**
7. **Directrices NNUU (1990)**

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

¿QUÉ ES UN DATO PERSONAL?

toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona identificable a toda persona cuya identidad pueda determinarse, directa o indirectamente en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, unos datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona

¿CUÁNDO UNA PERSONA ES IDENTIFICABLE?

Atención a factores objetivos, (costes y tiempo necesarios para la identificación, tecnología disponible o avances tecnológicos).

¿CUÁLES SON LAS CATEGORÍAS ESPECIALES DE DATOS?

Origen étnico o racial, opiniones políticas, religión, convicciones filosóficas, afiliación sindical, datos genéticos y biométricos (dirigidos a identificar de una manera unívoca a una persona), salud, vida y orientación sexual.

¿QUÉ ES UN TRATAMIENTO DE DATOS?

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

¿QUIÉN ES EL RESPONSABLE DEL TRATAMIENTO?

Persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o conjuntamente con otros determine los fines y los medios del tratamiento

¿QUIÉN ES EL ENCARGADO DEL TRATAMIENTO?

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

REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

PRINCIPALES CARACTERÍSTICAS

Mayor control para los interesados de sus datos

Nuevo modelo de cumplimiento basado en la responsabilidad proactiva

Enfoque de riesgos

Nuevo modelo de supervisión

Mecanismos de cooperación para su aplicación uniforme

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 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)**
- **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 la LOPDGDD)**
- **Datos de personas jurídicas**

EXCLUSIONES

- ✓ **Tratamiento efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas. Antecedentes:**
  - **Sentencia Lindqvist: "vida privada y familiar de los particulares".**
  - **No aplicación: videovigilancia si capta vía pública (Sentencia Ryneš)**

- ✓ **RGPD. Interpretación aparentemente restrictiva**

- ✓ **Ejercicio de "actividades exclusivamente personales o domésticas" (Cdo. 18)**
  - **Podrían incluir la correspondencia y la llevanza de un repertorio de direcciones, o la actividad en las redes sociales y la actividad en línea realizada en el contexto de dichas actividades personales y domésticas.**
  - **No obstante, el presente Reglamento debe aplicarse a los responsables o encargados del tratamiento que proporcionen los medios para tratar los datos personales relacionados con tales actividades personales o domésticas**

Redes sociales

- ✓ **Será preciso tener en cuenta el contexto de la actividad: comercial o privada. Pueden tenerse en cuenta criterios sobre perfiles abiertos o cerrados, pero no basados en límites cuantitativos (número de «amigos»)**
  - **Actividad privada (particular): responsabilidad del SRS propia de un servicio de intermediación. Similar, por ejemplo, a la de un buscador**
  - **Actividad comercial o empresarial: responsabilidad del usuario**

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"

PRINCIPIOS

Los principios se mantienen similares a la regulación anterior (Directiva/LOPD), reforzados en algunos aspectos

- **Licitud, lealtad y transparencia**
- **Minimización de datos**
- **Limitación de finalidad**
- **Exactitud**
- **Limitación del plazo de conservación**
- **Integridad y confidencialidad**
- **Responsabilidad proactiva**

PRINCIPIOS

- **Principio de licitud, lealtad y transparencia**
  - La transparencia o información como nuevo principio
- **Principio de limitación de finalidad**
  - Especialidades en el tratamiento para fines distintos (artículo 6.4)
- **Principio de minimización**
  - Reemplaza "no excesivos" con "limitados a lo necesario"
  - "Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios"
- **Principio de exactitud** (LOPDPGDD)
  - Facilitados por el propio afectado
  - Facilitados por intermediarios legalmente previstos
  - Recibidos como consecuencia del ejercicio del derecho a la portabilidad
- **Principio de limitación del plazo de conservación**
  - El plazo debe ser objetivo, pero puede no ser una fecha determinada o depender de la conducta del afectado
- **Principio de integridad y confidencialidad**
  - Seguridad y confidencialidad como principios y no como obligaciones
- **Principio de responsabilidad proactiva**

LICITUD DEL TRATAMIENTO

Art. 6.1

a) consentimiento para el tratamiento de sus datos personales para uno o más fines específicos

b) ejecución de un contrato en el que el interesado es parte o para la aplicación, a petición de éste, de medidas precontractuales

c) cumplimiento de una obligación legal a la que está sujeto el responsable del tratamiento

d) intereses vitales del interesado o de otra persona física

LICITUD DEL TRATAMIENTO

e) cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento

f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los derechos y libertades fundamentales del interesado que requieren la protección de los datos personales, en particular, cuando el interesado sea un niño. Ello no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones

CONSENTIMIENTO

Libre, específico, informado e "inequívoco" → A través de declaraciones o "claras acciones afirmativas"

Se considera que puede existir un acto afirmativo claro en supuestos como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal (Cdo. 32)

También puede considerarse acto afirmativo marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta

El silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento (Cdo. 32)

Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos (Cdo. 32)

No debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno (Cdo 42)

No debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibro claro entre el interesado y el responsable del tratamiento"(Cdo. 43)

Revocable tan fácil como prestarlo, sin efectos retroactivos

CONSENTIMIENTO

El consentimiento "tácito" o "por omisión" NO resulta conforme al RGPD, por lo que los tratamientos que se hayan basado en el "consentimiento tácito" deberían haber recabado un nuevo consentimiento ajustado al RGPD o ampararse otra causa de legitimación (en caso de responsables privados el interés legítimo previa ponderación de ese interés con la posible intrusión en los derechos y libertades de los afectados

Consentimiento de menores con autorización → 16 años, pudiendo los EEMM reducir la edad hasta 13 (LOPDPGDD 14 años)

En todo caso, el responsable deberá poder demostrar que cuenta con el consentimiento y que ha sido prestado por el afectado a través de los medios que resulten pertinentes

CAMBIO DE MODELO. CUANDO EXISTA OTRA BASE JURÍDICA PARA EL TRATAMIENTO NO DEBERÁ RECABARSE EL CONSENTIMIENTO

OBLIGACIÓN LEGAL- INTERÉS PÚBLICO

Cuando el tratamiento se fundamente en el cumplimiento de una obligación legal, el interés público o el ejercicio de potestades públicas, estas causas han de tener como base el derecho de la UE o de los EEMM

INTERÉS PÚBLICO (LOPDPGDD):

- **Videovigilancia**
- **Ficheros de exclusión publicitaria**
- **Denuncias internas**

INTERÉS LEGÍTIMO

…no será de aplicación ***al tratamiento realizado por las*** *autoridades públicas en el ejercicio de sus funciones* **(art. 6.1.f RGPD).**

Precisado por la Disposición adicional décima LOPDPGDD. *"Los responsables enumerados en el artículo 77.1 (sector público) podrán comunicar los datos personales que les sean solicitados por sujetos de derecho privado cuando cuenten con el consentimiento de los afectados o aprecien que concurre en los solicitantes un interés legítimo que prevalezca sobre los derechos e intereses de los afectados conforme a lo establecido en el artículo 6.1 f) del Reglamento (UE) 2016/679."*

INTERÉS LEGÍTIMO

Prácticamente similar a su configuración en la normativa anterior (Directiva 95/46/CE)

- **Especial referencia a tratamientos de niños y exclusión en el caso de autoridades públicas**
- **Algunos ejemplos de posibles intereses legítimos a valorar (no determina la prevalencia, sino sólo la existencia de intereses legítimos a tener en cuenta)**
  - **Prevención del fraude (si se cumple el principio de minimización)**
  - **Marketing directo**
  - **Transmisiones de datos dentro de Grupos empresariales para fines administrativos internos**
    - **Por ejemplo, centralización de datos de clientes o empleados**
  - **Transmisiones para garantizar la seguridad de las redes, por ejemplo a los CERT**
    - **Para impedir el acceso no autorizado a las redes de comunicaciones electrónicas y la distribución malintencionada de códigos, y frenar ataques de «denegación de servicio» y daños a los sistemas informáticos y de comunicaciones electrónicas**

INTERÉS LEGÍTIMO

Título IV LOPDPGDD

- **No es un *numerus clausus*. Pueden existir otros supuestos**
  - **Tanto en normas actualmente vigentes como en posibles habilitaciones legales futuras**
- **Tipologías**
  - **Supuestos en que se han tomado en consideración las especialidades del régimen de vigente**
    - **Datos de contacto de personas jurídicas necesarios para su localización profesional y para relacionarse con la persona jurídica**
    - **Datos de empresarios individuales**
    - **Solvencia**

CATEGORÍAS ESPECIALES DE DATOS

Nuevas categorías de datos

- **Datos genéticos**
  - **Datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona**
- **Datos biométricos**
  - **Datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos**

Aclaración: El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física (Cdo. 51)

CATEGORÍAS ESPECIALES DE DATOS

Regla general: QUEDA PROHIBIDO SU TRATAMIENTO

Excepciones a la prohibición

- **Consentimiento (LOPDPGDD precisa los datos en los que no es suficiente: ideología, afiliación, sindical, religión, orientación sexual, creencias, o étnico)**
- **Habilitación en el ámbito del derecho laboral y de seguridad o protección social (puede basarse en Convenio Colectivo)**
- **Tratamiento para la protección de intereses vitales del afectado o un tercero**
- **Datos manifiestamente públicos**
- **Tratamiento necesario por razones de Interés público esencial según la Ley UE o Nacional siempre que sea proporcional a la finalidad perseguida**
- **Defensa y reclamaciones y Tribunales**

CATEGORÍAS ESPECIALES DE DATOS

…//…

- **Medicina preventiva o laboral y evaluación de la capacidad laboral, diagnóstico médico o prestación sanitaria, gestión de los sistemas o servicios sanitarios. Exigencia de tratamiento llevado a cabo por profesional sujeto a deber de secreto o bajo su responsabilidad**
- **Razones de interés público en el ámbito de la salud pública, así como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios**
- **Archivo y fines de investigación histórica o científica o estadísticos en los términos del propio Reglamento**

DATOS DE INFRACCIONES Y SANCIONES

- **No están calificados como categorías especiales de datos (art. 10 RGPD y 27 LOPDPGDD)**
- **Su tratamiento exige (LOPDPGDD):**
  - **Ser órgano competente para procedimientos sancionadores y declaración de infracciones y sanciones**
  - **Limitado estrictamente a la finalidad del órgan**
- **Si no: consentimiento interesados o autorización por Ley**
- **Excepción: Abogados y procuradores cuyo objeto sea recoger la información facilitada por sus clientes**

DERECHOS

- Catálogo tradicional con tres novedades
  - Información
  - Acceso
  - Rectificación
  - Cancelación (derecho al olvido)
  - Limitación del tratamiento
  - Portabilidad
  - Oposición
- Previsiones sobre ejercicio de estos derechos
  - Lenguaje claro e inteligible
  - Obligación de “facilitar el ejercicio”
  - Plazos de respuesta → 1 mes
  - Formas de ejercicio → Posible vía electrónica
  - Gratuidad
  - Uso de iconos para proporcionar información

EL DERECHO/DEBER DE INFORMACIÓN

Se incrementa la información que habrá de facilitarse cuando los datos se recaban del afectado

- **Identidad y los datos de contacto del responsable y, en su caso, de su representante**
- **Datos de contacto del delegado de protección de datos**
- **Fines y base jurídica del tratamiento**
- **Intereses legítimos del responsable o de un tercero**
- **Destinatarios o las categorías de destinatarios de los datos personales, en su caso**
- **Transferencias internacionales previstas**

EL DERECHO/DEBER DE INFORMACIÓN

- **Plazo de conservación**
- **Derechos de acceso, rectificación o supresión, limitación del tratamiento, oposición y portabilidad**
- **Posibilidad de revocación del consentimiento**
- **Derecho a presentar una reclamación ante una autoridad de control**
- **Si la comunicación de datos personales es obligatoria y las posibles consecuencias de no facilitar los datos**

EL DERECHO/DEBER DE INFORMACIÓN

- **Existencia de decisiones automatizadas, incluida la elaboración de perfiles, la lógica aplicada y las consecuencias previstas**

Si los datos no se recaban del interesado deberá además informársele de:

- **Categorías de datos que se van a tratar**
- **Fuente de la que proceden los datos personales y, en su caso, si proceden de "fuentes de acceso público"**

EL DERECHO/DEBER DE INFORMACIÓN

Excepciones al deber de información

- **En general, cuando el interesado ya disponga de la información**

- **Si los datos no proceden del interesado cuando**
  - **Supongan un esfuerzo desproporcionado, en particular para fines de archivo, estadísticos o de investigación científica o histórica**
  - **Previsión legal expresa de tratamiento o revelación, con medidas oportunas de protección**
  - **Obligación de secreto legal o profesional**

EL DERECHO/DEBER DE INFORMACIÓN

Exigencia de claridad, concisión y fácil acceso (criterios AEPD: información por capas y por tablas)

LOPDPDGG (artículo 11)

- **Información básica:**
  - **Identidad del responsable y de su representante, en su caso**
  - **Finalidad del tratamiento**
  - **Modo de ejercer los derechos**
  - **En su caso:**
    - **Elaboración de perfiles**
    - **Posibilidad oponerse a las decisiones automatizadas**
- **Resto información mediante dirección electrónica en la que se pueda acceder a ella**

DERECHO DE ACCESO

Alcance

- **Confirmación de la existencia de tratamiento**
- **Acceso a los datos y a la información vinculada a los mismos**
  - **Fines**
  - **Categorías de datos**
  - **Categorías (al menos) de destinatarios**
  - **Plazo de conservación o criterios de fijación**
  - **Información de derechos de rectificación y supresión**
  - **Posibilidad de reclamación a la autoridad de control**
  - **Información disponible sobre el origen de los datos**
  - **Existencia de decisiones automatizadas o perfilado**
  - **Garantías adecuadas implantadas en caso de transferencia**

Modo de acceso: copia de los datos (y la información asociada)

- **Ampliación respecto del concepto tradicional de acceso, similar al de la LAP**
- **Gratuidad de la primera copia y canon orientado a costes en las ulteriores**
- **Uso de medios electrónicos si el derecho se ejercitó por ellos**

Restricción: perjuicio de derechos de terceros

Aclaraciones (considerando 63)

- **Posibilidad de satisfacer el acceso mediante acceso remoto seguro**
- **Posibilidad de que el responsable pueda pedir aclaración al interesado**

DERECHO A LA SUPRESIÓN "OLVIDO"

Revocación del consentimiento

- **"El interesado retire el consentimiento en que se basa el tratamiento y no tenga amparo en otro fundamento jurídico"**

Configuración tradicional del derecho de cancelación

- **"Los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo"**
- **"Los datos personales hayan sido tratados ilícitamente"**
- **"Los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento"**

Derecho de oposición

- **"El interesado se oponga al tratamiento con arreglo al artículo 21.1 (situación particular y tratamiento al amparo 6.1.e y f) y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21.2 (mercadotecnia directa)"**
  - **Inversión de la carga de acreditación del "interés legítimo imperioso" (art. 21)**

Datos de menores de edad que se hayan obtenido en relación con la oferta de servicios de la sociedad de la información (art. 8.1)

DERECHO A LA SUPRESIÓN "OLVIDO"

Supresión de enlaces

- Cuando el responsable haya hecho públicos los datos y proceda la supresión
- Obligación de informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos
- Límites: tecnología disponible y coste de su aplicación

Excepciones

- Ejercicio de las libertades de expresión e información
- Cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento,
- Tratamiento para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable
- Razones de interés público en el ámbito de la salud pública
- Fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, en la medida en que el derecho pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento
- Formulación, ejercicio o defensa de reclamaciones

RECTIFICACIÓN Y OPOSICIÓN

DERECHO DE RECTIFICACIÓN

- **Vinculación directa con el carácter inexacto o incompleto de los datos**

DERECHO DE OPOSICIÓN

- **General**
  - **Basado en motivos relacionados con la situación personal del afectado (art. 21.1)**
  - **Cuando el tratamiento se basa en el interés público, ejercicio de potestades públicas o el interés legítimo**
  - **Inversión de la prueba: será el responsable el que deberá justificar "motivos imperiosos para el tratamiento" que prevalezcan sobre los derechos de los afectados**
- **Opt-out en marketing directo**
  - **Sin necesidad de especificar ningún motivo concreto**
  - **Obligación de especificación concreta y separada del derecho en la primera comunicación comercial que se le dirija**
  - **Posibilidad de ejercicio en todo caso a través de medios automatizados**
- **Opt-out en caso de tratamiento con fines de investigación y estadísticos por motivos relacionados con su situación particular, salvo que el tratamiento lo sea por razones de interés público**

LIMITACIÓN DEL TRATAMIENTO

Concepto: “marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro”.

Naturaleza: diferencias con el bloqueo de los datos

- **Derecho del afectado vs. obligación legal del responsable**

Supuestos

- **Equivalentes a la “cancelación cautelar”**
  - **“El interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos”**
  - **“El interesado se haya opuesto al tratamiento en virtud del artículo 21.1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado”**
- **Por voluntad del afectado**
  - **“El tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso”**
  - **“El responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones”**

DERECHO A LA PORTABILIDAD

Derecho del interesado a

- **Recibir los datos personales que le incumban,**
- **Que haya facilitado a un responsable del tratamiento,**
- **En un formato estructurado y de uso habitual y de lectura mecánica**
- **Y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable del tratamiento al que se hubieran facilitado los datos**

Requisitos para que pueda ejercitarse (acumulativos):

- **El tratamiento esté basado en el consentimiento o en un contrato**
- **El tratamiento se efectúe por medios automatizados**

DERECHO A LA PORTABILIDAD

Modo de ejercicio

- **Podrá implicar la transmisión directa de responsable a responsable a instancia del interesado "cuando sea técnicamente posible"**

Limitaciones

- **Exceptuado cuando el tratamiento se funde en el cumplimiento de una misión de interés público o inherente al ejercicio del poder público. Difícil aplicación en las AAPP**

¿Qué dicen las autoridades europeas de protección de datos?

- **Aplicación a datos facilitados directamente o resultado del funcionamiento, pero no a los datos inducidos**

OTROS DERECHOS

DECISIONES AUTOMATIZADAS

- **Referencia expresa a la elaboración de perfiles**
- **Derecho a no ser objeto de una decisión que "produzca efectos" sobre el afectado o "le afecte significativamente de modo similar"**
- **Excepciones**
  - **Vinculación a contrato**
  - **Autorización por el derecho Nacional o de la UE**
  - **Consentimiento explícito**
- **Salvo en caso de habilitación legal, el interesado tiene derecho a obtener intervención humana en la decisión y que el interesado pueda dar su opinión e impugnar la decisión**
- **Salvo que exista consentimiento o interés público, no podrá implicar datos sensibles**

Obligación de comunicación de la rectificación, supresión o limitación del tratamiento a los cesionarios

RESPONSABLE-ENCARGADO

- **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"**

RESPONSABLE-ENCARGADO

- **Autorización, específica o general, previa información para recurrir a otro encargado/subencargado del tratamiento. Si es general el encargado informará al responsable para oposición, en su caso. Garantías contractuales (Cloud computing: subencargado del tratamiento)**

- **Asistirá al responsable, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados: acceso, oposición, rectificación, cancelación, limitación, portabilidad, decisiones automatizadas**

- **Ayudará al responsable a garantizar el cumplimiento de las obligaciones sobre seguridad del tratamiento, brechas de seguridad, evaluaciones de impacto y consulta a la AEPD**

- **Pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.**

RESPONSABLE-ENCARGADO

LOPDPGDD (Disposición transitoria quinta)

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.

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

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

- **LOPDPGDD:**
  - **inclusión de la base jurídica**
  - **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

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

· REGISTRO DE ACTIVIDADES DEL RGPD

ADMINISTRACIÓN LOCAL (responsables de tratamiento)	ENCARGADOS DE TRATAMIENTO DE LA ADMINISTRACIÓN LOCAL
Nombre y datos de contacto del responsable (o representante).	Nombre y datos de contacto del encargado (o representante).
Fines del tratamiento	Categorías de tratamientos efectuados por cuenta de cada responsable
Nombre y datos de contacto del Delegado de Protección de Datos.	Nombre y datos de contacto del Delegado de Protección de Datos.
Categorías de datos personales.	.....
Categorías de afectados.	.....
Descripción de las medidas técnicas y organizativas de seguridad.	Descripción de las medidas técnicas y organizativas de seguridad.
Categorías de destinatarios de comunicaciones, incluidos terceros países u organizaciones internacionales.	
Transferencias internacionales. Documentación de garantías adecuadas en caso del 49.1.	Transferencias internacionales. Documentación de garantías adecuadas en caso del 49.1.
Cuando sea posible, plazos previstos para las supresión de las diferentes categorías de datos.	.....

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

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

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

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/orientación sexual**

PRIVACIDAD desde el DISEÑO

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 ciudadano 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

Variara en función de

- **Los tipos de tratamiento**
- **La naturaleza de los datos**
- **El número de afectados**
- **La cantidad y variedad de tratamientos que s realicen**
- **(www.aepd.es) HERRAMIENTA FACILITA**
- **(www.aepd.es) GUÍA DE ANÁLISIS DE RIESGOS**
- **(www.aepd.es) LISTADO DE CUMPLIMIENTO NORMATIVO**
- **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

MEDIDAS DE SEGURIDAD

LOPDPGDD

DISPOSICIÓN ADICIONAL PRIMERA. MEDIDAS DE SEGURIDAD EN EL ÁMBITO DEL SECTOR PÚBLICO

El Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos personales, para evitar su pérdida, alteración o acceso no autorizado.

Los responsables enumerados en el artículo 77.1 deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad.

En los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad.

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

- **(www.aepd.es) GUÍA SOBRE EVALUACIONES 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

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 y se deja al ámbito interno la fijación del sector público);**
- **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

LOPDPDGG INCLUYE SUPUESTOS QUE RESPONDEN A LOS REQUISITOS RGPD (art. 34), entre otros:

- **Colegios profesionales y sus consejos generales**
- **Centros educativos y universidades públicas y privadas**
- **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**
- **…**

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 privacidad desde el diseño y por defectos, 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 deja 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**
  - **Titulación**
  - **Acreditación**
- **Esquema de certificación de ENAC**

DELEGADO DE PROTECCIÓN DE DATOS

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**
- **No es aplicable el régimen sancionador de la LOPDPGDD a los DPD (art. 70.2)**
- **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 la Autoridad de Control, salvo que sea improbable que constituya un riesgo para los derechos y libertades de las personas

Plazo: sin dilación indebida y a más tardar en 72 horas

Contenido mínimo:

- Naturaleza de la quiebra de seguridad: categorías de afectados (por ejemplo: menores, discapacitados, empleados, ciudadanos), núm. aproximado de afectados, categorías de datos comprometidos (por ejemplo: identificativos, salud, laborales)…
- Nombre y datos de contacto del DPD
- Posibles consecuencias de la quiebra de seguridad sufrida
- Medidas adoptadas o propuestas para remediar esta quiebra

Necesario establecer protocolos para gestionar y notificar las quiebras de seguridad

BRECHAS DE SEGURIDAD

COMUNICACIÓN A LOS INTERESADOS: necesaria cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, salvo si:

- Se han adoptado y aplicado medidas sobre los datos personales afectados, particularmente aquellas que hagan ininteligibles los datos para cualquier persona que no esté autorizada a acceder ellos (por ejemplo: se han cifrado los datos personales)
- El responsable ha adoptado medidas ulteriores que garanticen que ya no existe un alto riesgo para los derechos y libertades
- Que la comunicación supusiese un esfuerzo desproporcionado, optándose por una comunicación pública o medida semejante por la que se informe de forma efectiva a los afectados

Los entes de la Administración Local pueden elaborar un **Plan de Contingencias** con la finalidad de mitigar los daños cuando se produzca una quiebra de seguridad. También deben mantener un **registro de los incidentes de seguridad**

(www.aepd.es) 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 INTERNACIONALES DE DATOS

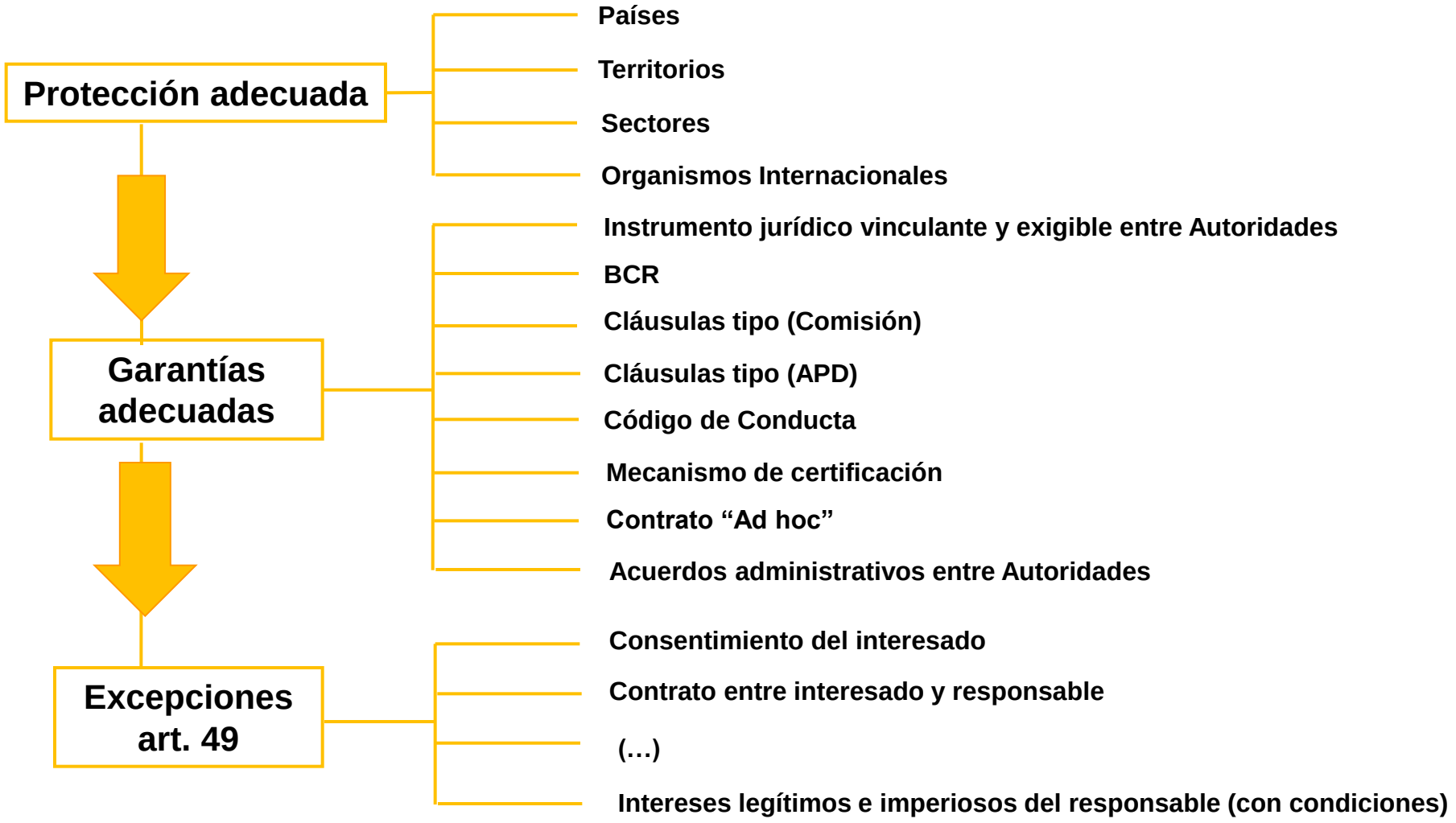
Se mantiene aproximación europea clásica → TID sólo posibles si:

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

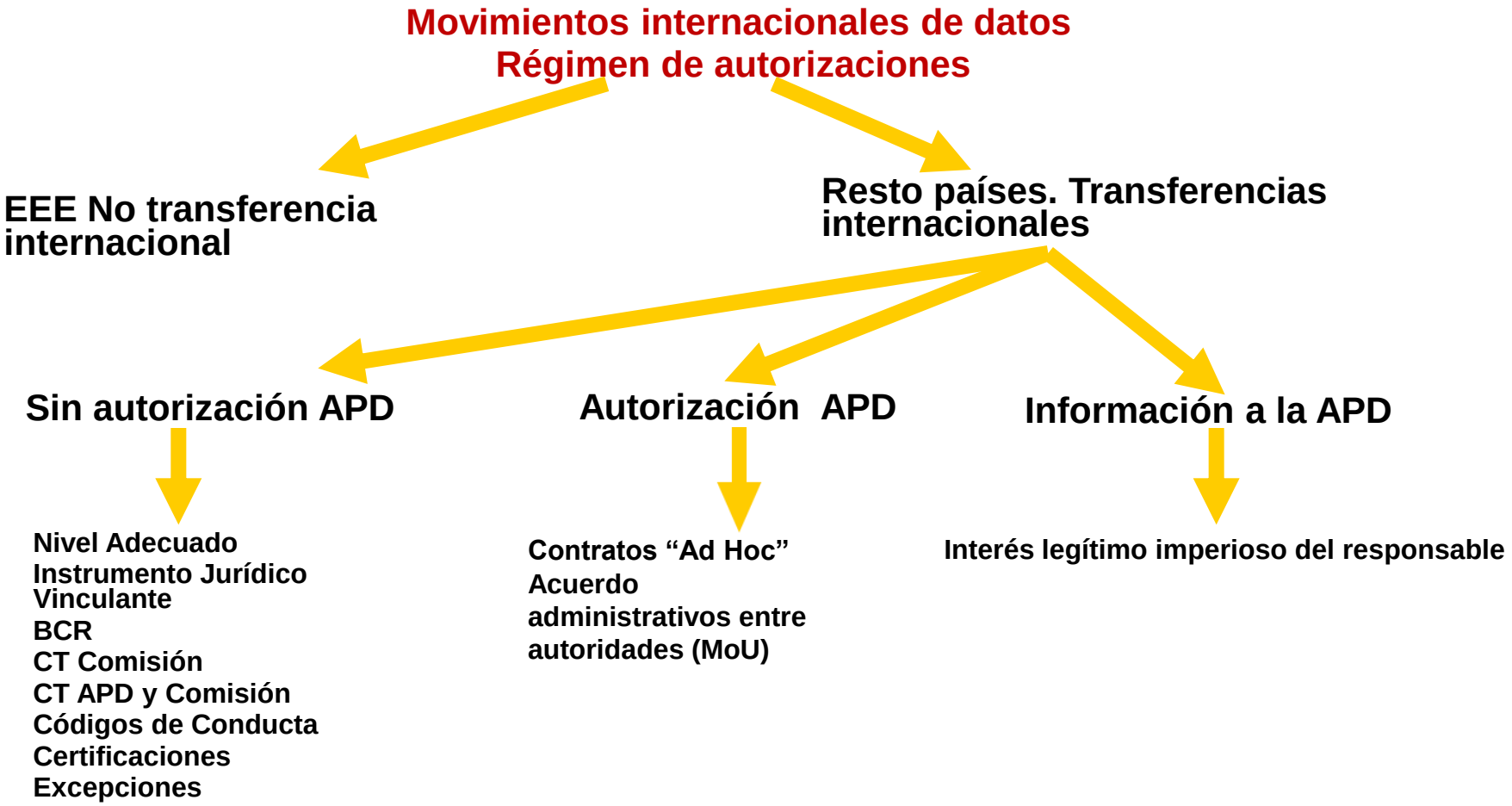
TRANSFERENCIAS INTERNACIONALES DE DATOS

- **Con autorización previa de APD →**
  - **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



TRANSFERENCIAS INTERNACIONALES DE DATOS



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)

DECISIONES DE ADECUACIÓN ADOPTADAS POR LA COMISIÓN EUROPEA (RGPD)

Japón (24.01.19)

MODELO DE SUPERVISIÓN

- **Acciones correctivas →**
  - **Sancionar con una advertencia cuando las operaciones de tratamiento previstas puedan infringir RGPD**
  - **Sancionar con apercibimiento cuando las operaciones de tratamiento hayan infringido RGPD**
  - **Ordenar al responsable o encargado del tratamiento que atiendan las solicitudes de ejercicio de los derechos**
  - **Ordenar que las operaciones de tratamiento se ajusten a las disposiciones del RGPD, de una determinada manera y dentro de un plazo especificado**
  - **Ordenar al responsable que comunique al interesado las violaciones de la seguridad de los datos personales**
  - **Imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición**

MODELO DE SUPERVISIÓN

- **Multas deberán ser efectivas, proporcionadas y disuasorias**
- **Cantidad deberá modularse atendiendo a circunstancias del caso**
- **Aplicables a responsables y encargados**
- **Clasificación de infracciones y sanciones**
    - **Multa hasta 10 M € o para empresas, optándose por la de mayor cuantía, hasta el 2 % de volumen de negocio anual a nivel mundial**
        - **Obligaciones de responsable o encargado**
        - **Obligación de organismos de certificación**
        - **Obligaciones de los organismos de supervisión de códigos de conducta**

MODELO DE SUPERVISIÓN

- **Multa hasta 20 M € o hasta el 4%**
  - **Principios básicos**
  - **Derechos**
  - **Transferencias internacionales**

- **Multa hasta 20 M € o hasta el 4%**
  - **Incumplimiento de resoluciones de APD**

MODELO DE SUPERVISIÓN

SUJETOS RESPONSABLES (art.70 LOPDPGDD)

- Responsables del tratamiento
- Encargados del tratamiento
- Representantes de responsables o encargados fuera UE
- Entidades de certificación
- Entidades de supervisión códigos de conducta acreditadas
- Excluidos los DPD

PRESCRIPCIÓN DE INFRACCIONES: 3 años las muy graves, 2 las graves y 1 las leves

PRESCRIPCIÓN DE SANCIONES: 3 33 años + de 300.000 €, 2 años, entre 40.001 y 300.000 €, y 1 año hasta 40.000 €

La AEPD podrá remitir las reclamaciones al DPD y, en su caso al responsable antes de admitirlas a trámite para que den respuesta en un mes.

Las AAPP no serán objeto de sanciones económicas (se mantiene el régimen de la LOPD)

RÉGIMEN SANCIONADOR PARA EL SECTOR PÚBLICO (art.77.1 LOPDGDD)

- ***Sanción de apercibimiento** con medidas para corregir los efectos de la infracción*
- ***Notificación al responsable o encargado del tratamiento, al órgano jerárquicamente superior, en su caso, y a los afectados***
- ***Propuesta de actuaciones disciplinarias** en caso de indicios suficientes para ello*
- ***En infracciones imputables a autoridades o directivos, en las que no se hayan atendido informes técnicos o recomendaciones, se incluirá una amonestación con denominación del cargo y publicación en el BOE o Diario Oficial autonómico***
- ***Se comunicará al Defensor del Pueblo y se publicará en la web de la AEPD***

TAREAS DE ADAPTACIÓN AL REGLAMENTO

agencia española protección datos

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

LOPDPGDD

- **Incorporar al Derecho nacional previsiones interpretación RGPD y completar sus disposiciones. Complemento del RGPD**
- **Regulación datos personas fallecidas (art.3)**
- **Se fija en 14 años la edad para prestar el consentimiento (art. 7)**
- **Regula tratamientos concretos (datos de contacto empresarios, sistemas de información crediticia, sistemas de exclusión publicitaria, denuncias internas, videovigilancia, solvencia,…)**
- **Bloqueo de los datos en caso de rectificación o supresión para la exigencia de responsabilidades durante su plazo de prescripción. Disponibles sólo para jueces, tribunales, M. Fiscal y AAPP (art.32)**
- **Relación de entidades que requieren DPD y su papel para resolver conflictos en protección de datos (art. 34 y 65.4)**
- **El Régimen de la AEPD**
- **El régimen sancionador (Título IX)**

LOPDPGDD

- **Reconocimiento derechos digitales (neutralidad de la Red, acceso universal, desconexión digital, educación digital, etc. Título X)**
- **Medidas de seguridad en los tratamientos de las AAPP: el Esquema Nacional de Seguridad (D.A. 1ª)**
- **Inclusión en ficheros de morosos por deudas de más de 50 € (D.A. 6ª)**
- **Potestad de las AAPP para verificar sin necesidad de consentimiento la exactitud de los datos personales (D.A. 8ª)**
- **Derecho ciudadanos a no aportar documentos a las AAPP cuando obren en ellas. Las AAPP pueden consultarlos salvo que se opongan a ello, excepto en potestades sancionadoras o de inspección (D.F. 12ª)**
- **Modificaciones leyes sectoriales (jurisdicción contenciosa, transparencia sanidad, educación…)**

DISPOSICIÓN ADICIONAL SÉPTIMA

- **Identificación de interesados en notificaciones por medio de anuncios y publicaciones actos administrativos:**
  - **Acto administrativo: nombre y apellidos y 4 cifras aleatorias (DNI, NIE), alternas si se refiere a una pluralidad de afectados**
  - **Anuncios DNI y si no tiene nombre y apellidos: nunca juntos**
  - **Especial cuidado para casos de violencia de género**

LOPDPGDD

ORIENTACIONES PROVISIONALES AEPD/AVPD/APDCAT/CTPDA

Criterio provisional propuesto para tratar de evitar que la adopción de fórmulas distintas en aplicación de la citada disposición pueda dar lugar a la publicación de cifras numéricas de los documentos identificativos en posiciones distintas en cada caso, posibilitando la recomposición íntegra de dichos documentos (completo en www.aepd.es).

La publicación de documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente podrá realizarse de la siguiente forma:

- **Dado un DNI con formato 12345678X, se publicarán los dígitos que en el formato que ocupen las posiciones cuarta, quinta, sexta y séptima. En el ejemplo: ***4567**.**
- **Dado un NIE con formato L1234567X, se publicarán los dígitos que en el formato ocupen las posiciones, evitando el primer carácter alfabéticos, cuarta, quinta, sexta y séptima. En el ejemplo: ****4567*.**
- **Dado un pasaporte con formato ABC123456, al tener sólo seis cifras, se publicarán los dígitos que en el formato ocupen las posiciones, evitando los tres caracteres alfabéticos, tercera, cuarta, quinta y sexta. En el ejemplo: *****3456.**

LOPDPGDD

- **Dado otro tipo de identificación, siempre que esa identificación contenga al menos 7 dígitos numéricos, se numerarán dichos dígitos de izquierda a derecha, evitando todos los caracteres alfabéticos, y se seguirá el procedimiento de publicar aquellos caracteres numéricos que ocupen las posiciones cuarta, quinta, sexta y séptima. Por ejemplo, en el caso de una identificación como: XY12345678AB, la publicación sería: *****4567*****
- **Si ese tipo de identificación es distinto de un pasaporte y tiene menos de 7 dígitos numéricos, se numerarán todos los caracteres, alfabéticos incluidos, con el mismo procedimiento anterior y se seleccionarán aquellos que ocupen las cuatro últimas posiciones. Por ejemplo, en el caso de una identificación como: ABCD123XY, la publicación sería: *****23XY.**

Los caracteres alfabéticos, y aquellos numéricos no seleccionados para su publicación, se sustituirán por un asterisco por cada posición.

SE RECOMIENDA QUE LA FÓRMULA PROPUESTA SEA APLICADA DE FORMA GENERALIZADA

TRATAMIENTOS DE DATOS EN LA ADMINISTRACIÓN LOCAL

PREGUNTAS FRECUENTES

Padrón de habitantes
Pleno y Concejales
Publicación de datos
Tratamiento de datos en el marco laboral
Videovigilancia
Acceso a expedientes administrativos y transparencia
Otras cuestiones

GUÍA PROTECCIÓN DE DATOS Y ADMINISTRACIÓN LOCAL

www.aepd.es

agencia española protección datos

MUCHAS GRACIAS

www.aepd.es

@AEPD_es