

PRIVACIDAD



UN DERECHO FUNDAMENTAL



SEGURdades

Consultores en protección de datos personales

SEGURdades  
es el asesor  
de su entidad  
en materia de  
protección de  
datos.

Nuestro  
objetivo es  
formarles en  
la materia  
de  
protección  
de datos.

Aclarar  
conceptos  
y sus  
obligaciones  
como  
usuarios.



LA PRIVACIDAD, UN DERECHO FUNDAMENTAL



# INDICE

1. Bien jurídico y sujeto protegido
2. Contexto histórico
3. Conceptos básicos
4. Principios
5. Obligaciones de los usuarios
6. Otra normativa con incidencia



# 1. BIEN JURÍDICO Y SUJETO PROTEGIDOS



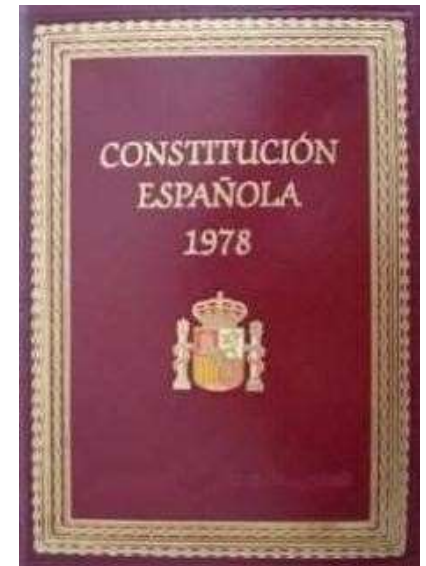
de la persona física



# 1.1. LA PRIVACIDAD

- Comprende la esfera más restringida de nuestra vida
- En España es recogida por la Constitución por el derecho a la intimidad:

*“Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen” – art. 18.1 Constitución Española*



## 1.2.OBJETIVO DE LA REGULACIÓN LEGAL

- Reconocer un **derecho inherente** a la persona
- Proteger la libre configuración y **desarrollo de la personalidad**
- Brindar **garantías** para su protección



## 2. CONTEXTO HISTÓRICO

En el s. XXI utilizamos los datos personales para realizar:

CADA VEZ MENOS



SE ALMACENAN  
MANUALMENTE



SOLICITUDES
INSCRIPCIONES
CONTRATACIONES
COMPRAS
RECIBIR OFERTAS

CADA VEZ MÁS



SE ALMACENAN  
DIGITALMENTE

## 2.1.EVOLUCIÓN HISTÓRICA

SISTEMA DE TRATAMIENTO DE DATOS	PERÍODO	REGULACIÓN
	AÑOS 60	Países nórdicos: para evitar los abusos en el tratamiento masivo España: art 18.1 CE
	AÑOS 90	España: LORTAD del 1992 Europa: Directiva UE 95/46,





## 2.1.EVOLUCIÓN HISTÓRICA

	AÑO 2000	España: LOPD 15/1999 RD 1720/2007
	AÑO 2016	Europa: Reglamento UE 2016/679 (RGPD)
	AÑO 2018	España: LOPDGDD 3/2018



## 2.2.MARCO REGULATORIO ACTUAL



Unificar las  
normas europeas



Proteger los datos privados  
de sus ciudadanos



## 2.2.MARCO REGULATORIO ACTUAL

### AMBITO MATERIAL

- ✓ Datos personales
- ✓ Personas físicas
- ✓ Tratamiento total o parcialmente automatizado



### AMBITO TERRITORIAL

- ✓ Responsable se encuentre en al UE.
- ✓ Interesado sea ciudadano de la UE.
- ✓ Responsable no se encuentre un lugar externo a la UE pero en el que aplique el derecho de la UE.



## 2.2.MARCO REGULATORIO ACTUAL


### Excepciones a la aplicación del RGPD

- ✘ Ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de UE.
- ✘ Ejercicio de actividades exclusivamente personales o domésticas de personas físicas.
- ✘ Tratamiento de datos de personas fallecidas, sin perjuicio de lo establecido en el art. 3 LOPDGDD



## 2.2.MARCO REGULATORIO ACTUAL

### Excepciones a la aplicación del RGPD

- ✘ Actividades de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención.
- ✘ Tratamientos sometidos a la normativa sobre protección de  clasificadas.

# 3. CONCEPTOS BÁSICOS

- 3.1. Dato personal
- 3.2. Tratamiento
- 3.3. Responsable del tratamiento
- 3.4. Encargado del tratamiento
- 3.5. Usuario
- 3.6. Delegado de protección de datos



# 3. CONCEPTOS BÁSICOS: ¿qué es un dato personal?

*Aquella información que identifica o puede identificar a una persona que es el **interesado***

- NOMBRE / APELLIDO
- DIRECCIÓN
- NÚMERO DE TELÉFONO
- IMAGEN
- CORREO ELECTRÓNICO
- NÚMERO DE LA SEGURIDAD SOCIAL

**NOTA:** la denominación de interesado en esta presentación no es la misma que la de la Ley 30/2015 de Procedimiento Administrativo Común



# Categorías de datos de la Administración

- De carácter identificativo
- De carácter tributario
- De carácter académicos y profesionales
- De la ejecución de la potestad sancionadora
- De categorías especiales
- De la implantación de las 'Smart Cities'





### 3. CONCEPTOS BÁSICOS: ¿qué significa “tratamiento” de datos?

*Cualquier operación realizada a los datos personales ya se automatizada o no*

- ✓ RECOGIDA
- ✓ COPIA
- ✓ MODIFICACIÓN
- ✓ EXTRACCIÓN
- ✓ ACCESO
- ✓ COMUNICACIÓN
- ✓ DIFUSIÓN
- ✓ CONSERVACIÓN
- ✓ DESTRUCCIÓN



# Tipos de tratamiento en la Administración

- Padrón municipal de habitantes
- Subvenciones y ayudas
- Sanciones
- Obras y licencias
- Policía Local
- Gestión de Tributos
- Bolsa de Trabajo
- Cementerio municipal
- Recursos Humanos
- Servicios Sociales
- Gestión económica



### 3. CONCEPTOS BÁSICOS: ¿quién es el responsable del tratamiento ?

*El **responsable** es la persona física o jurídica que define el motivo por el que se pueden tratar datos y los medios para realizar dicho tratamiento*



### 3. CONCEPTOS BÁSICOS: ¿quién es el encargado del tratamiento ?



*En cambio el **encargado** es la persona física o jurídica que trata los datos por cuenta del responsable y bajo sus ordenes.*

*¿Y si utiliza los datos para otros fines? Dejará de ser encargado y será responsable.*



# 3.CONCEPTOS BÁSICOS: ¿quién es el usuario de los datos?



Los empleados como todas aquellas personas que intervenimos en el tratamiento de los datos POR

EJEMPLO para:

- Pedir el currículum en una entrevista
- Copiarlos a un programa nuevo
- Enviarlos a otra empresa
- Eliminarlos en la destructora

# 3. CONCEPTOS BÁSICOS: ¿quién es el Delegado de Protección de Datos?

Es la persona (jurídica o física) que tiene como obligación el buen cumplimiento de la legislación. Es conocido como DPD o DPO (Data Protection Officer):



- ✓ Puede ser alguien de la plantilla o un externo a la empresa.
- ✓ Deberá tener conocimientos jurídicos y, en materia de protección de datos.
- ✓ Será obligatorio para ciertas entidades (art 37 del RGPD)

NH1



# 4.Principios

4.1. Licitud

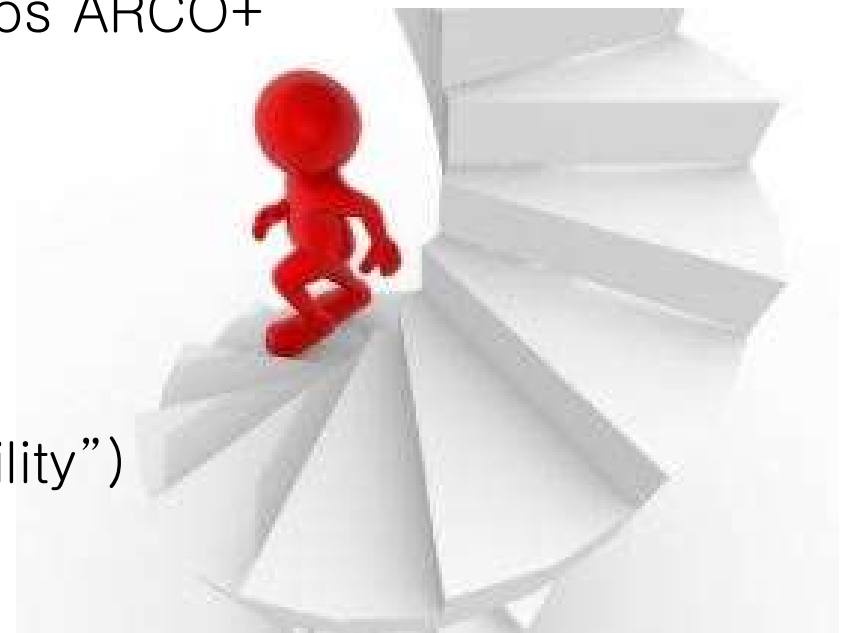
4.2. Derecho de la información: derechos ARCO+

4.3. Intervención mínima

4.4. Limitación finalidad

4.5. Conservación

4.6. Rendición de cuentas (“accountability”)



## 4.1. Principios: **licitud**

a) Consentimiento **expreso** (no tácito) del interesado:

Ej. **Aceptar la casilla de condiciones de registro de usuario**



b) Ejecución de un contrato:



Ej. **El tratamiento de nombre, dirección y cuenta bancaria por ENDESA**

c) Por obligación legal del responsable:

Ej. **Hacer copia DNI de los huéspedes de alojamientos turísticos.**





d) Por interés vital del interesado u otra persona física

Ej. Nombre de los empleados afectados por el COVID-19



e) Misión realizada en interés público o en el ejercicio de poderes públicos concedidos al responsable

Ej. El certificado negativo de delitos Sexuales para trabajar en un colegio



f) En interés de intereses legítimos del responsable o de un tercero

Ej. La instalación de cámaras de seguridad



# Consentimiento expreso

**NOTA:** la LOPDGDD establece la edad mínima de 14 años para prestar el consentimiento

En todo caso mediante una acción clara ‘de hacer’.

## EJEMPLO

SI  NO  acepto a recibir comunicaciones por SMS

---

YO..... Con DNI .....acepto a que el Ayuntamiento.....utilice mis datos para comunicarse vía SMS en relación a la petición realizada.

Firma:



## 4.2 Principios: derecho a la información

- ✓ La identidad del responsable
- ✓ El contacto del DPO
- ✓ La finalidad del tratamiento
- ✓ El interés legítimo si lo hay
- ✓ Los destinatarios o categoría de destinatarios
- ✓ La intención de transferir datos a un tercer país u organización
- ✓ Plazo de conservación de los datos



# Principales medios de recogida de datos

En toda aquella mediante la cual se recaben datos personales sea en formato papel como por medios digitalizados:

- 1) Instancias/Formularios
- 2) Facturas
- 3) Solicitudes
- 4) Páginas web
- 5) Correos electrónicos
- 6) Teléfono



- ✓ La posibilidad de ejercer los **derechos ARCO+**
- ✓ La posibilidad de **retirar el consentimiento** cuando el tratamiento sea lícito por
- ✓ El derecho de presentar **reclamación** ante la autoridad de control
- ✓ Si **la comunicación** de datos personales es **un requisito legal o contractual** y de las consecuencias de no facilitar dichos datos
- ✓ La existencia de **decisiones automatizadas**



DERECHOS ARCO+
ACCESO
RECTIFICACIÓN
SUPRESIÓN
OPOSICIÓN
LIMITACIÓN
PORTABILIDAD DE LOS DATOS

# Protección de Datos y Transparencia

- Diferencia entre el acceso a los datos por el mismo interesado y el acceso a la información pública por cualquier ciudadano.
- La Ley de Transparencia no nos permite hacer público o difundir toda aquella información que también pueda contener datos personales
- Especial relevancia cuando dicha información pueda contener datos de carácter especial (art.9 del RGPD).



# Supuestos más frecuentes

## 1– Solicitud de acceso a expedientes administrativos por un tercero

- En caso de expedientes abiertos: solo tendrá acceso a dicha información aquellos que sean partes interesadas en el procedimiento (Ley de Procedimiento Administrativo Común).
- En caso de expedientes finalizados: podrá tener acceso cualquier persona en base a la Ley de Transparencia con límites. Se deberán omitir los datos de carácter especial. Los datos meramente identificativos podrán ser omitidos cuando no sea relevante para el solicitante (bajo ponderación).



# Supuestos más frecuentes

## 2-Solicitud de acceso a documentación de la Administración por la oposición

- La ley de Bases de Régimen Local permite dicho acceso siempre que la información sea tratada por la oposición bajo las funciones propias de éste y no más allá.
- En consecuencia, la oposición no podría difundir dicha información o utilizarla para otros fines distintos.
- Excepción sobre la información tributaria (art. 95 de la Ley General Tributaria).





# Supuestos más frecuentes

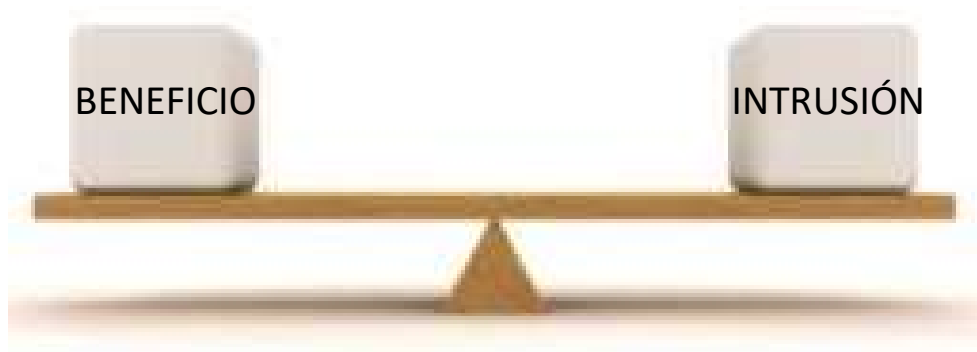
## 3- Publicación o difusión de datos relativos a empleados por los sus órganos de representación

- La ley del Estatuto Básico del Empleado público establece en el art. 40 las competencias del órgano de representación.
- Éste no podrá difundir datos de un empleado sin el consentimiento expreso de dicho empleado.
- El órgano de representación no tiene derecho a copia del contrato de un empleado en concreto (a no ser que exista consentimiento expreso) sino a copia básica y por tanto sin datos personales



## 4.3.Principios: **intervención mínima**

- **Finalidad**: se consigue la finalidad deseada
- **Proporcionalidad**: hay otros medios menos intrusivos a la intimidad
- **Juicio de valor** entre



**EJEMPLO 1.** La instalación de un sistema de audiovisual de seguridad en una oficina

- 1.La finalidad de control de incidencias de seguridad se cumple
- 2.Con solo videovigilancia se podrían controlar eventuales incidencias
- 3.El beneficio de seguridad resulta menor que el sacrificio a la intimidad de los trabajadores



**EJEMPLO 2.** Registro de visitas para acceder a las oficinas de la empresa

- 1.La finalidad de control de accesos con fines de seguridad
- 2.No existe otro medio menos intrusivo para controlar a las visitas en unas oficinas tan relevantes
- 3.El beneficio de seguridad resulta mayor que el sacrificio de la visita a aportar nombre completo y DNI.



## 4.3.Principios: **limitación**

Los datos personales deben ser recogidos para fines:

✓ Determinado

✓ Explícitos

✓ Legítimos

✗ No distintos a los originales



**CASO 1** Utilizar el correo electrónico de un cliente para para enviar promociones



**CASO 2.** Utilizar el correo electrónico de un cliente para informarle sobre una incidencia sobre su pedido



## 4.4.Principios: **minimización de datos**

Los datos que se recogen deben de ser:



✓ pertinentes

✓ limitados

✗ no recabar más datos de los necesarios

Volviendo al ejemplo de control de visitas en las oficinas:

Nombre completo + DNI seria pertinente

**PERO NO número de teléfono o correo electrónico**



## 4.5.Principios: **conservación**



Los datos se deben conservarse **no más del tiempo legalmente exigido.**

Nunca indefinidamente

Esto dependerá de las finalidades de los datos:

- CONTABILIDAD
- RECURSOS HUMANOS
- CONTRATACIONES
- SEGURIDAD
- ETC.



## 4.5.Principios: **rendición de cuentas**

- El responsable debe ser **proactivo** y no reactivo, **previniendo**.

**¿Cómo?:** Estableciendo y aplicando medidas técnicas y organizativas para dar cumplimiento a las normas pudiendo demostrarlo



**AUDITORIAS**

**PERIODICAS**



# 5.Obligaciones de los usuarios

5.1.Contraseñas

5.2.Papel

5.3.Programas y sistemas

5.4.Notificación de violaciones  
de seguridad

5.5.Secretos profesionales

**¿Qué  
debo hacer?**



# 5.1.Obligaciones: contraseñas

Tener una contraseña de acceso en todos los soportes que almacenen datos personales sean de trabajadores como de clientes:

Ordenadores

Tablets

Móviles

Programas



Cambiarlas una vez al año

Y NO anotarlas

en un post it

enganchado a la pantalla



Que sean algo

elaboradas Y NO:



## 5.2.Obligaciones: papel

Guardar la documentación en mobiliario no accesible a nadie que no este autorizado



No dejar a la vista documentación cuando se atiende al público

Destruir la documentación en la destructora de papel o por empresa certificada



## 5.3.Obligaciones: programas y sistemas

- ✓ Utilizar los programas que nos facilita la empresa.
- ✗ Desconfiar de programas gratuitos.
- ✗ No utilizar dispositivos personales para trabajar.
- ✗ No conectar dispositivos personales a los de la empresa.
- ✓ Hacer un uso exclusivamente laboral del sistema de la empresa.
- ✗ No crear bases de datos externas a los programas sin autorización.



## 5.4.Obligaciones: **notificar violaciones de seguridad**



### SUPUESTOS:

¿Qué es una violación de seguridad?

Cualquier hecho que destruya, modifique o cause la pérdida de datos personales de forma **accidental** o **ilícita**

1. La pérdida/robo de un USB con datos personales de trabajadores o clientes
2. Deshacerse de documentos en la basura sin destruir
3. El funcionamiento anormal de los sistemas o programas
4. La falta de documentos sobre algún expediente



## 5.4.Obligaciones: **notificar violaciones de seguridad**

¿A quién se la comunico?

Al superior directo de la empresa, informático/a, al Delegado de Protección de Datos o asesor en la materia.



¿De que debo informar?

De lo que ha pasado y de la categoría de datos personales que se vean afectados: volumen y número de afectados si es posible



¿Con que rapidez?

Lo antes posible para valorar el perjuicio ocasionado y notificar a la autoridad de control en menos de 72h desde que se tiene conocimiento

## 5.5.Obligaciones: guardar secreto profesional

No difundir datos de trabajadores o clientes a nadie de fuera de la empresa a excepción del mismo interesado.



Ante la petición por parte de un tercero para acceder a datos se evaluará la idoneidad del supuesto y si se estima se redactara un contrato de confidencialidad



# 6. Otra normativa con incidencia

- 6.1. RD 311/2022, de 3 de mayo, por el que se regula el **Esquema Nacional de Seguridad (ENS)**
- 6.2. Ley 34/2002 sobre los **Servicios de la Sociedad de la Información y el Comercio Electrónico**
- 6.3. Ley Orgánica 1/1982 sobre protección civil al derecho al honor, la intimidad personal y familiar y a la **propia imagen**





# 6.1 Esquema Nacional de Seguridad (ENS)



## SUJETO OBLIGADO

Administración Pública

## OBJETIVO

- Establece la política de la seguridad en la utilización de medios electrónicos (art.42 de la Ley 11/2007)
- Proteger la Seguridad de la Información en los medios de las tecnologías de la Información



## 6.2 Ley sobre los Servicios de la Sociedad de la Información y el Comercio Electrónico

### SUJETO OBLIGADO

Personas jurídicas que tengan la sede social en España o sucursales u oficinas en ella desde donde gestionen la prestación de servicios en Internet

### OBJETIVO

Regulación de actividades económicas por Internet u otros medios telemáticos.

Lista la información que se debe facilitar al consumidor: información de la empresa, sobre el proceso de compra y el derecho de desistimiento.

**IMPORTANTE:** art 21.1 sobre correos electrónicos y 22.2 sobre cookies



## 6.3 LO sobre protección civil al derecho al honor, la intimidad familiar y a la propia imagen

### SUJETO OBLIGADO

Toda persona física

### OBJETIVO

Proteger los derechos reconocidos en el art 14 de la Constitución

### IMAGEN

Es necesario el consentimiento expreso de la persona para la captación y/o publicación de su imagen

#### Excepciones art 8.2:

1. Cargos públicos o personajes de cierta notoriedad en lugares o actos públicos.
2. La imagen sea accesoria a otra
3. El uso de caricaturas



# CONCLUSIONES

- 1 CUMPLIR CON NUESTRAS OBLIGACIONES
- 2 COMUNICAR CUALQUIER INCIDENCIA O SOSPECHA
- 3 ANTE SOBRE COMO DEBEN TRATARSE LOS DATOS, PREGUNTAR



# Para más información consultar:

ORIENTACIÓN A LAS ADMINISTRACIONES PÚBLICAS

<https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/directrices-de-aplicacion/administraciones-publicas>

DECÁLOGO ADAPTACIÓN AL RGPD DE LA ADMINISTRACIÓN PÚBLICA

<https://www.aepd.es/sites/default/files/2019-09/infografia-adaptacion-rgpd-aapp.pdf>





# SEGURdades

Consultores en protección de datos personales

[info@segurdades.com](mailto:info@segurdades.com)

Tel. 902360842

LA PRIVACIDAD, UN DERECHO FUNDAMENTAL



GRACIAS

