

# RGPD

TODO LO QUE NECESITA SABER  
PARA SUS CAMPAÑAS



spot **hit**

Su plataforma de **marketing**

● ● Pilotar de manera sencilla sus campañas multicanal

# ÍNDICE DE CONTENIDOS DE ESTE DOCUMENTO

## **4** INTRODUCCIÓN

## **6** DERECHOS DE LAS PERSONAS INTERESADAS

- Derecho de acceso
- Derecho de rectificación
- Derecho a la portabilidad
- Derecho al olvido/derecho de supresión
- Derecho de oposición
- Revocación del consentimiento
- Obligación de notificación
- Algunas aclaraciones

## **10** CARTOGRAFÍA DE LOS DATOS

- ¿Quién...?
- ¿Qué...?
- ¿Por qué...?
- ¿Dónde...?
- ¿Hasta cuándo...?
- ¿Cómo...?
- La CNIL (*Comisión Nacional de Informática y Libertades francesa*) le ayuda

## **14** RECOGIDA DE LOS DATOS PERSONALES

- Finalidad de la recogida de los datos
- Marco de la recogida del consentimiento de las personas

## 18 SUBCONTRATACIÓN

---

## 20 SEGURIDAD

---

- Proteger los locales
- Asegurar los puestos de trabajo
- Proteger las redes informáticas
- Asegurar los servidores
- Proceso de copia de seguridad y continuidad de actividad
- Supervisar el mantenimiento y la destrucción de los datos
- Asegurar los intercambios externos

## 22 CERTIFICACIÓN

---



# INTRODUCCIÓN

A pesar de que esta nueva legislación europea parece ser un freno para sus estrategias de marketing, tiene como objetivo ofrecer mayor control y transparencia a los consumidores.

Es fundamental abordarla como un medio de crear una relación de confianza con sus clientes.



## **RGPD**

Reglamento General de  
Protección de Datos



## **GDPR**

General Data  
Protection Regulation

## **OBJETIVO**

Armonizar la regulación de los datos personales en todo el territorio europeo.

## **¿POR QUÉ ESTA LEY?**

- Legislación obsoleta.
- Aumento del volumen de recogida y tratamiento de los datos personales.
- Falta de controles y sanciones concretas.

## ¿CÓMO?

Tres años de negociaciones entre las tres principales instituciones europeas: Parlamento Europeo, Consejo de la Unión Europea y Comisión Europea.

## ¿PARA CUÁNDO?

25 de mayo de 2018.

Para esa fecha, debe poder demostrar que ha comenzado a adoptar las medidas para el cumplimiento del reglamento.



## ¿PARA QUIÉN?

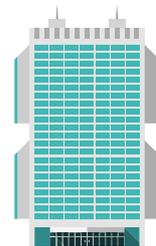
Todos los organismos que realizan tratamientos de datos personales en la Unión Europea en el marco de su actividad profesional.

## MULTAS

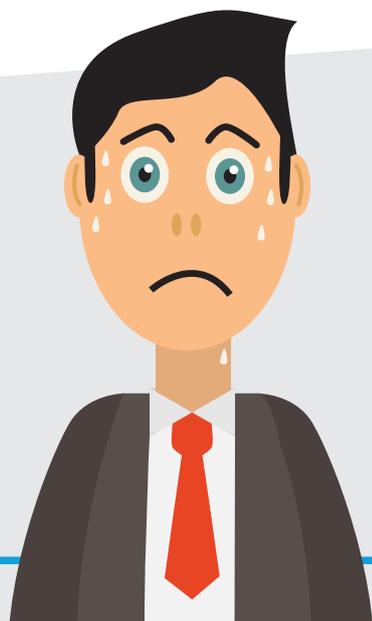
En lo referente a las infracciones más graves, las sanciones son muy disuasivas :



**20 millones de euros**  
para las PYME y los  
organismos públicos



**4 % del VN del grupo**  
para las grandes empresas



## ¡NO SE ASUSTE!!

Antes de alcanzar estos importes considerables, la ley prevé llamadas al orden y multas más modestas. Estas se establecen teniendo en cuenta la transgresión efectuada y el nivel de colaboración con la CNIL.

# DERECHOS DE LAS PERSONAS INTERESADAS

Esta nueva ley tiene como principal objetivo aumentar los derechos de las personas interesadas que han compartido sus datos personales.

Encontrará, pues, a continuación la lista y las modalidades de aplicación de los diferentes derechos.

## 1 DERECHO DE ACCESO



La persona interesada tienen derecho al acceso a los datos que usted ha recogido.

Le puede solicitar, entre otras cosas, los siguientes datos: las finalidades, las categorías de datos que posee, las personas o entidades que tienen acceso a esta información, etc.



**Para más información**

<https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre3#Article15>

## DERECHO DE RECTIFICACIÓN

2

Sus contactos pueden modificar los datos recogidos inexactos y pueden solicitar que se completen los datos incompletos.



**Para más información**

<https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre3#Article16>

## 3 DERECHO A LA PORTABILIDAD

Sus contactos pueden exportar (o solicitarle) todos los datos que ha recogido y que les conciernen.

Idea: Espacio destinado en su sitio internet, que permita a sus clientes llevar a cabo esto con autonomía para evitarle perder el tiempo.



**Para más información**

<https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre3#Article20>

## DERECHO AL OLVIDO / DE SUPRESIÓN

4



Sus contactos pueden solicitar, en todo momento y en un plazo de tiempo breve, que se supriman todos sus datos personales.

En algunas circunstancias, usted está autorizado a rechazar la supresión de los datos personales. Sin embargo, si la persona interesada lo solicita, se verá obligado a limitar las finalidades del tratamiento.



**Para más información**

<https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre3#Article17>  
<https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre3#Article18>

## 5 DERECHO DE OPOSICIÓN

Las personas interesadas tienen derecho a oponerse al tratamiento de sus datos. Sin embargo, el responsable puede rechazar este tratamiento si demuestra motivos legítimos e imperiosos que justifiquen el tratamiento.



**Para más información**

<https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre3#Article21>

## 6 REVOCACIÓN DEL CONSENTIMIENTO

Sus contactos tienen derecho a revocar su consentimiento en todo momento. Usted tiene que poner a su disposición un medio sencillo para llevar a cabo la solicitud.

## OBLIGACIÓN DE NOTIFICACIÓN

7

Ha de informar a sus contactos en los siguientes tres casos: rectificación, supresión o restricción.

Sin embargo, puede eludir esta obligación si prueba que esta es imposible de llevar a cabo o requiere un esfuerzo desproporcionado.



### Para más información

<https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre3#Article19>

## 8 ALGUNAS ACLARACIONES



### 1. Identidad de la persona interesada

Usted tiene derecho a exigir a las personas interesadas que proporcionen una prueba de identidad.

### 2. Plazo para cumplir con los derechos de las personas interesadas

Si tiene un número de solicitudes muy elevado o estas son muy complejas, puede prorrogar este plazo dos meses adicionales.



### 3. Gastos relativos a las solicitudes de las personas interesadas

En el caso de individuos que intentan ejercer estos derechos de forma abusiva, usted está autorizado a facturar gastos razonables por «solicitudes repetitivas», «solicitudes manifiestamente infundadas o excesivas» o por «ejemplares adicionales».





### Para más información

<https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre3#Article12>

<https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre3#Article13>

<https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre3#Article14>

# INFORMACIÓN DETALLADA



# CARTOGRAFÍA DE LOS DATOS

Es uno de los elementos de la documentación solicitada por la norma, que consiste en responder a preguntas sencillas que delimitan el tratamiento de los datos personales dentro de su organismo.

A continuación encontrará los diferentes puntos en cuestión :

## 1 ¿QUIÉN...?

### 1. ¿Quién es el responsable del tratamiento de los datos personales en su empresa?

Designe un responsable encargado de decidir sobre el tratamiento de los datos o un «Delegado de Protección de Datos» (DPD) en función de su situación :

	REFERENTE	DPD
Tratamiento de los datos normales*	✓	✓
Tratamiento de los datos sensibles*	✗	✓
PYME**	✓	✓
Autoridades / organismos públicos**	✗	✓
Obligación de declaración a la CNIL***	✗	✓



- \* <https://www.cnil.fr/fr/definition/donnee-sensible>
- \*\* <https://www.cnil.fr/fr/devenir-delegue-la-protection-des-donnees>
- \*\*\* <https://www.cnil.fr/fr/designez-en-ligne-votre-delegue-la-protection-des-donnees-aupres-de-la-cnil>

## 2. ¿Qué personas estarán obligadas a tratar datos personales dentro de su organización?

Puede tratarse de personas designadas en función de su actividad, posición jerárquica o incluso de sus competencias.

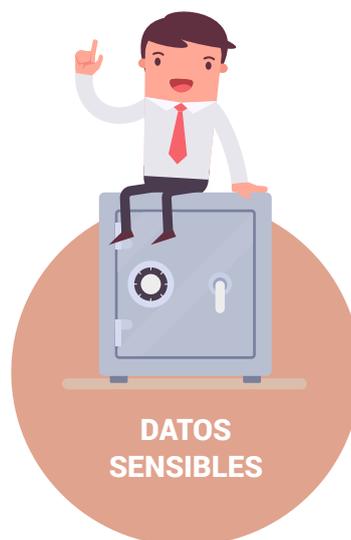
## 3. ¿Quiénes son los subcontratistas que tienen acceso a los datos personales de sus clientes?

Ver la sección «Subcontratistas».

# 2 ¿QUÉ...?

## ¿Qué categorías de datos recoge su empresa?

Categorice las tipologías de datos.



## ¿Qué es un dato sensible?

Información sobre el origen racial o étnico, las opiniones políticas, filosóficas o religiosas, la pertenencia sindical, la salud o la vida sexual. En principio, únicamente se pueden recoger y explotar los datos sensibles con el consentimiento explícito de las personas.

Fuente : <https://www.cnil.fr/fr/definition/donnee-sensible>

# ¿POR QUÉ...?

# 3

## ¿Con qué finalidad recoge usted los datos de sus clientes?

Determine los objetivos de su recogida de datos.

**Ejemplo :** gestión de la clientela, encuesta de satisfacción, operación de fidelización.



Cuidado, el tiempo de conservación varía en función de las necesidades.

**Ejemplo :** cuando se realiza un pago con tarjeta bancaria, únicamente se conservan los datos bancarios durante la duración del pago.

## 4 ¿DÓNDE...?

¿Dónde se encuentran alojados sus datos? ¿Por dónde transitan sus datos?

La duración de conservación varía en función de la naturaleza de los datos y de las finalidades perseguidas

## ¿HASTA CUÁNDO...?

5

¿Durante cuánto tiempo debe conservar los datos recogidos?

La duración de conservación varía en función de la naturaleza de los datos y de las finalidades perseguidas durante la recogida.

### DURACIÓN DE LA CONSERVACIÓN



**ARCHIVOS CORRIENTES**  
Base activa

**ARCHIVOS INTERMEDIARIOS**  
(acceso restringido, etapa intermedia antes de eliminación)

**ARCHIVOS DEFINITIVOS**  
(datos con un interés histórico, estadístico, que justifica su no destrucción)

En concreto, un dato únicamente debe conservarse durante el tiempo de duración del logro del objetivo inicial.

Ejemplo: datos personales con finalidades comerciales : máximo 3 años.



**Más información**

<https://www.cnil.fr/fr/limiter-la-conservation-des-donnees>

## 6 ¿CÓMO...?

### ¿Cómo se tratan los datos una vez que los ha recogido?

Implemente procesos de seguridad para minimizar los riesgos y limitar los accesos para evitar cualquier impacto sobre la vida privada de las personas interesadas.

Ejemplo: seguridad en los puestos de trabajo: bloqueo automático de las sesiones/instalación de un cortafuego/multiplicar las copias de seguridad.

## LA CNIL LE AYUDA 7



# RECOGIDA DE LOS DATOS PERSONALES

Lo que está abocado a desaparecer para proteger a las personas interesadas :



**Casillas marcadas**



**La recogida de datos  
sin límite**



**La recogida de datos  
pasiva**

## El aumento de los datos personales

Datos que hasta el día de hoy no estaban considerados como datos personales, ahora sí lo están, como las cookies y los datos de localización.

## 1 FINALIDAD DE LA RECOGIDA DE LOS DATOS

### 1. Indique de forma clara sus objetivos de recogida

Tal y como hemos visto en la sección «¿Por qué?» de la cartografía de los datos, es importante determinar las finalidades, pero también es fundamental indicarlas con claridad a las personas interesadas.

Cada casilla para marcar de sus formularios tendrá que especificar, por lo tanto, la finalidad y el soporte utilizado para esta comunicación.

### 2. Se debe respetar la finalidad

En el caso de que el tratamiento de los datos personales no corresponda con el uso que ha indicado en el momento de la recogida, las personas interesadas tendrán derecho a solicitar el olvido o la oposición de sus datos.

# MARCO DE LA RECOGIDA DEL CONSENTIMIENTO DE LAS PERSONAS



## 1. Las prácticas que se deben implementar

Obligación de obtener una respuesta clara, precisa e inequívoca de las personas en relación a la recogida de su consentimiento.

## 2. Limitar los datos recogidos

Únicamente se deben recoger los datos que tienen una relación directa con la finalidad. Para evitar cualquier error que podría ocasionar solicitudes de derecho al olvido, más vale solicitar únicamente la información principal.

Los siguientes son algunos ejemplos y contraejemplos de recogida de datos :

<p> Acepto recibir la newsletter mensual por CORREO ELECTRÓNICO.</p> <p> Acepto recibir SMS concretos en función de mis datos de navegación.</p> <p> Acepto recibir ofertas puntuales por SMS (descuentos, promociones...)</p> <p> Acepto recibir la revista trimestral. Campos que se deben cumplimentar: dirección postal, apellido, nombre.</p> <p> Acepto las CGV (ventana emergente que recoge los casos mencionados).</p>	<p> Acepto recibir todas las semanas la newsletter, así como ofertas específicas.</p> <p><b>&gt; Prohibición de utilizar una casilla para recopilar los consentimientos para varias finalidades; y no se especifica el canal.</b></p> <p> En el caso de que no desee recibir ofertas comerciales, marque la casilla.</p> <p><b>&gt; Prohibición de utilizar una casilla desmarcada como acto de consentimiento.</b></p> <p> Acepto recibir la revista trimestral/campos que se deben cumplimentar: dirección de correo electrónico, móvil, dirección postal, apellido, nombre.</p> <p><b>&gt; Prohibición de recogida de información que no esté relacionada con la finalidad.</b></p> <p> Acepto las CGV y doy mi consentimiento para el tratamiento de mis datos personales.</p> <p><b>&gt; Prohibición de mezclar las CGV y un tratamiento de los datos no detallados.</b></p>
	

### 3. Cree nuevas menciones legales

En sus campañas, redirija a sus clientes o potenciales clientes hacia menciones legales especiales «Tratamiento de los datos», con las que demuestra que la confidencialidad de los datos es una de sus principales preocupaciones.



1. Presente a la persona a cargo del tratamiento de los datos en su estructura e indique el modo de contactar con ella.
2. Informe a sus clientes sobre su derecho a revocar su consentimiento, proponiendo unos pasos a seguir sencillos y rápidos.

### 4. No olvide la cancelación de la inscripción

Además de todos los cambios aportados por la norma, no olvide continuar aplicando las buenas prácticas. Siempre tendrá la obligación de ofrecer a sus destinatarios la posibilidad de darse de baja de sus campañas.



Por ello, piense en utilizar las listas de exclusión e integrar los medios de cancelación de inscripción presentes en nuestra herramienta.



#### Más información

<https://www.cnil.fr/fr/comprendre-vos-obligations/les-principes-cles>



# SUBCONTRATACIÓN

Cuando sus datos transitan fuera de su organismo, la responsabilidad recae sobre usted. Por lo tanto, es fundamental que aplique un proceso completo para garantizar a sus clientes subcontratistas «cumplidores».



## Recurrir únicamente a subcontratistas que presenten garantías

Debe exigir a los proveedores interesados un documento que detalle su política de tratamiento de los datos personales, denominado «Registro de los tratamientos». Esto le permitirá comprobar los conocimientos y la implicación del proveedor en este tema.

## Implementar medidas de seguridad

En colaboración con sus subcontratistas, deberá aplicar algunas medidas :

- Cifrado de los datos según su sensibilidad.
- Cifrado de las transmisiones de datos (HTTPS, VPN...).
- Garantías en materia de protección de la red, trazabilidad, autenticación.



## Modificar sus contratos

Es preferible formalizar los compromisos del proveedor en los contratos para poder demostrar que está recurriendo a proveedores cumplidores.

- Definir con claridad el objeto, la finalidad del tratamiento y las obligaciones.
- Inscriba restricciones mínimas en materia de autenticación.
- Defina las condiciones de restitución/ destrucción de los datos al final del contrato.
- Determine las normas de gestión y notificación en el caso de incidente con los datos personales.

**CONTRACT**

An illustration showing a pair of hands holding a pen and signing a document. The word 'CONTRACT' is written in bold, slanted letters above the document.

SPOT-HIT cumple con las exigencias del RGPD.

Se puede acceder a nuestro «Registro de los tratamientos» en todo momento :

[www.spot-hit.fr](http://www.spot-hit.fr)



Más información

<https://www.cnil.fr/fr/securite-gerer-la-sous-traitance>

## EJEMPLO DE CLÁUSULAS PARA ESTABLECER CON SUS SUBCONTRATISTAS

<https://www.cnil.fr/fr/sous-traitance-exemple-de-clauses>



# SEGURIDAD

Informar a los colaboradores sobre las obligaciones y expectativas del RGPD



## Proteger los locales

- Alarmas.
- Detectores de humo.
- Distinga las zonas de riesgo de sus locales (establecer un listado de las personas autorizadas en función de las zonas).
- Haga un listado de las entradas/salidas de las salas altamente aseguradas.

## Asegurar los puestos de trabajo

- Bloqueo de sesión con contraseña sólida.
- Cortafuego.
- Antivirus (actualizado con regularidad).



## Proteger las redes informáticas

- Gestionar las redes WIFI con un cifrado (WIFI o WPA2-PSK).
- Separar las redes abiertas para los invitados de la red interna.
- Limitar los flujos de red filtrando flujos entrantes/salientes.

## Asegurar los servidores

- Aplicar el protocolo TLS u otro protocolo que permita cifrar la autenticación.





## Proceso de copia de seguridad y continuidad de actividad

- Copias de seguridad frecuentes y si es posible en un lugar externo.
- Proteger las copias de seguridad (cifrado).
- Instaurar un plan de reanudación y continuidad de actividad informática.
- Prever una redundancia de los materiales, sobre todo de almacenamiento.

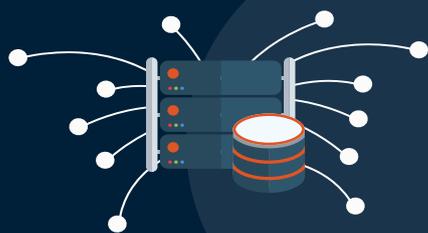
## Supervisar el mantenimiento y la destrucción de los datos

- Dejar constancia de las intervenciones en un registro (si el mantenimiento lo efectúa un organismo externo, ver la sección «Subcontratistas»).
- Instaurar un proceso de supresión segura de los datos (por ejemplo, supresión de los datos contenidos en un ordenador antes de enviarlo a reparar).



## Asegurar los intercambios externos

- Cifrar los datos.
- Utilizar un protocolo que garantice la seguridad (HTTPS, SFTP...).
- Ejemplo: si envía datos por correo electrónico, cifrelos y envíe la contraseña por un canal distinto (SMS...).



### Más información

<https://www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles>

# CERTIFICACIÓN



Serán los organismos autorizados por la CNIL o acreditados por el COFRAC (organismo nacional francés de acreditación) quienes expidan las certificaciones.

## Tenga cuidado con las «propuestas» de acreditaciones.

Como en el caso de todas las novedades, van acompañadas de un «efecto moda» que puede, potencialmente, llevar a empresas poco escrupulosas a proponer certificaciones sin valor.

¡Recorra a organismos serios y reconocidos!



### Para más información

<https://www.cnil.fr/fr/transition-vers-le-rgpd-des-labels-la-certification>

# CONCLUSIÓN

## Una reforma de dos niveles

Este nuevo reglamento se ha pensado, inicialmente, para proteger a los usuarios de los gigantes como Facebook o Google. El nivel de exigencias se adaptará, evidentemente, a cada tipología de empresa.

Usted deberá ser pragmático en la implementación de los diferentes procesos y proceder por etapas en función de en qué puntos ya ha avanzado más o menos.

## Un proceso a largo plazo

La fecha límite del 25 de mayo de 2018 no tiene por finalidad que usted haya llevado a cabo el cumplimiento al 100 %.

Su objetivo es que pueda probar que tiene conocimiento de los métodos que se deben implementar, que se ha tomado la norma en serio y que ha iniciado el cumplimiento.

# HOJA DE RUTA

Para ayudarle a evaluarse, le ofrecemos una hoja de ruta que le permitirá valorar su cumplimiento.

ETAPA  
**1**

## DESIGNAR UN PILOTO

Para pilotar la gobernanza de los datos personales de su estructura, necesitará un auténtico jefe de orquesta, que ejercerá una misión de información, asesoramiento y control internamente.

ETAPA  
**2**

## CARTOGRAFIAR

Para medir con exactitud el impacto del reglamento europeo en la protección de los datos que usted trata, empiece por identificar de manera precisa qué tipo de operaciones de tratamiento de datos lleva a cabo.

ETAPA  
**3**

## PRIORICE

Sobre la base de su registro, identifique las acciones necesarias para llevar a cabo el cumplimiento de las obligaciones actuales y futuras.

ETAPA  
**4**

## GESTIONE LOS RIESGOS

Si ha identificado tratamientos de datos personales susceptibles de engendrar riesgos elevados, deberá hacer un análisis de impacto a la privacidad (PIA) de cada uno de estos tratamientos.

ETAPA  
**5**

## ORGANIZAR

Para asegurar un alto nivel de protección de los datos personales permanentemente, establezca procedimientos internos que incorporen la protección de los datos en todo momento.

ETAPA  
**6**

## DOCUMENTAR

Para demostrar su cumplimiento con el reglamento, debe constituir y agrupar la documentación necesaria.

Para finalizar, a pesar de que esta documentación sobre el nuevo reglamento europeo de tratamiento de los datos personales es completa, no sirve como documento oficial.

Por lo tanto, puede ser útil solicitar un asesoramiento externo para confirmar la validez de sus buenas prácticas, por ejemplo, un despacho de abogados especializados.



Su plataforma de **marketing**  
Pilotar de manera sencilla sus campañas multicanal



SMS / MMS



VOZ



EMAIL



CORREO



BASE DE DATOS

Prueba gratis en

**spot-hit.es**



spot-hit.es



0800 73 44 20



info@spot-hit.es

Nota de difusión :

Autorizamos la difusión en la web de este documento con la condición de incluir sistemáticamente un enlace a [www.spot-hit.es](http://www.spot-hit.es).