Protección de Datos

Las obligaciones de protección de datos y su impacto en el día a día: Impacto del RGPD (Reglamento General de Protección de Datos) en sistemas y procedimientos.

DICIEMBRE 2019

Preocupaciones en torno a la protección de datos

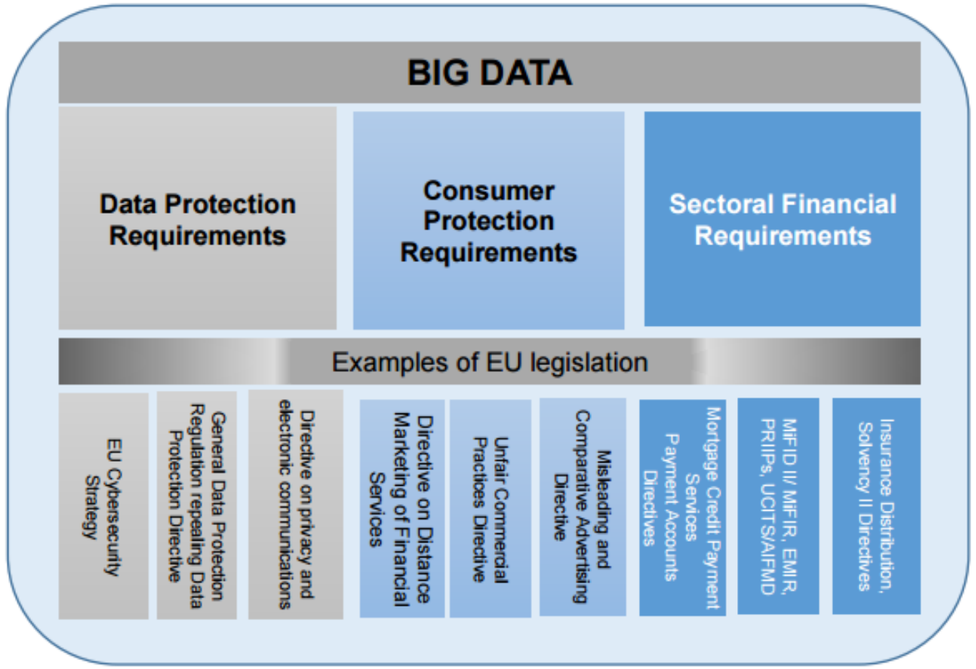
Las necesidades de protección de datos se han incrementado en estos últimos años de forma masiva. Por ello surgen nuevas preocupaciones compartidas por diferentes organismos:

- √ **Globalización** del uso de **internet** por todos los usuarios.
- √ **Internacionalización** de los datos (es necesario “alinear” las regulaciones de las **diferentes jurisdicciones**).
- √ Los datos a controlar cada vez son **más heterogéneos**.
- √ Los datos que se recogen son **cada vez más “personales”**, pues el usuario es un **contribuyente activo** (y a veces involuntario) de datos en cualquier momento y lugar.
- √ Los **usuarios** tienen una **mayor conciencia de la seguridad y la privacidad**, con gran inquietud porque las **empresas o gobiernos puedan controlar lo que se hace** en internet (53,8% de usuarios “**muy preocupados**” por las empresas, y 52,8% por los gobiernos, según una encuesta de 2015 de AIMC).
- √ La **constante innovación** provoca que requiera cada vez **más tiempo y** skills identificar si las compañías, con sistemas cada vez más complejos, emplean correctamente los datos.
- √ Necesidad de que los **profesionales TIC conozcan** estas materias y **asuman que los desarrollos tecnológicos que realicen respeten** los derechos de los ciudadanos.

Qué regulaciones vigilan los datos…

Los datos están inevitablemente controlados por múltiples regulaciones, y es una preocupación que va mucho más allá del Reglamento de Protección de Datos…

EL EJEMPLO DEL SECTOR FINANCIERO



Consulta Diciembre de 2016: Documento de Preguntas y Repuestas de 2016 de diferentes supervisores europeos sobre Big Data.

QUÉ PREOCUPA

- *Malas prácticas de mercado…*
- *No permitir el acceso a herramientas que se basen únicamente en la disponibilidad de un número elevado de datos.*
- *Políticas de privacidad muy vagas con "expresiones genéricas y poco claras", que obliga a acceder a multitud de enlaces".*
- *Limitaciones de tecnologías relacionadas con el Big Data por su menor nivel de desarrollo y madurez respecto a otras tecnologías tradicionales.*
- *Ser capaz de tratar los datos de forma estandarizada y qué todos los participantes del mercado reporten del mismo modo la información para poder mantener procedimientos de control.*

Qué regulaciones vigilan los datos…

Los datos están inevitablemente controlados por múltiples regulaciones, y es una preocupación que va mucho más allá del Reglamento de Protección de Datos…

SI BIEN SE IDENTIFICAN POTENCIALES BENEFICIOS….

- *Reducción de costes…*
- *Permitir un mejor acceso a la información a los clientes.*
- *Fomentar la Innovación"*
- *Mayor facilidad para detectar el fraude y otras actividades ilegales.*
- *Mejorar el cumplimiento regulatorio al facilitar la automatización y el control sistemático.*
- *Incremento de beneficios por un mejor uso de la información de clientes.*

LA NOVEDAD PUEDE PROVOCAR CIERTA "PREOCUPACIÓN" EN LOS ORGANISMOS SUPERVISORES / REGULADORES

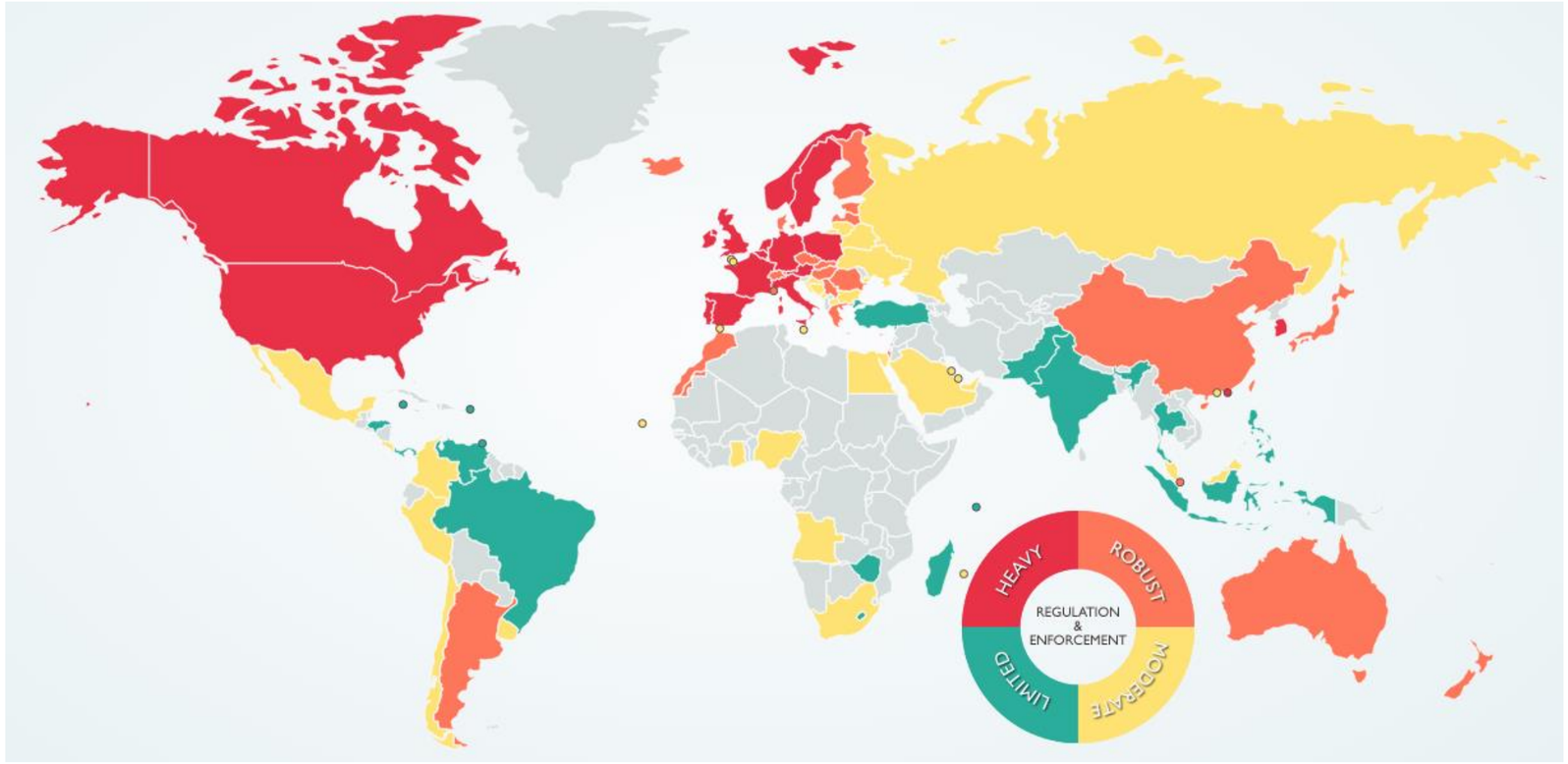
Existe preocupación por:

- *El desconocimiento de estos sistemas*
- *Potenciales daños reputacionales.*
- *Impacto en servicios que requieren dedicar tiempo al cliente y una cierta especialización: Por ejemplo, quejas y reclamaciones de los usuarios (tratamientos automatizados en vez de dar el servicio más adecuado al cliente).*
- *Riesgos de ciberseguridad y otros que pueden amplificarse.*
- *Posible crecimiento "descontrolado" de estos servicios.*

Consulta Diciembre de 2016: Documento de Preguntas y Repuestas de 2016 de diferentes supervisores europeos sobre Big Data.

Regulaciones de Protección de datos en el mundo

A modo ilustrativo, se muestra un mapa que muestra la fortaleza de las distintas regulaciones de protección de datos en los diferentes países:



En un entorno con cada vez más sanciones…

Las consecuencias de un incumplimiento de la Ley de Protección de Datos son claras y afectan incluso a las empresas más avanzadas… **Sanciones que se van a MULTIPLICAR con la entrada en vigor del nuevo RGPD.**

		CAUSAS	
	***Protección de Datos multa con 1,2 millones de euros a Facebook por usar datos personales sin permiso***	*- **No se informa adecuadamente** del uso de las **cookies**. - No se obtiene **consentimiento** del usuario. - **Políticas** de privacidad muy vagas con "expresiones **genéricas** y poco claras", que obliga a acceder a multitud de enlaces". - **No elimina la información** que recoge de los hábitos de navegación.*	SEPT. 2017
	***La AEPD multa a Google con 300.000 euros por Street View***	*- Captó y almacenó **sin consentimiento** datos personales de los ciudadanos procedentes de redes inalámbricas mediante vehículos de su proyecto Street View - Recabó, entre otra, información de e-mails, códigos de usuario y contraseña para acceder a buzones, direcciones IP, direcciones MAC de routers... (la mayor parte no son especialmente protegidos, pero no podían captarse ni siquiera de WIFI abiertas).*	NOV. 2017
	***Condena por el uso de "supercookies" en móviles sin obtener consentimiento (20.000 euros)***	*- Empleo de técnica de "supercookie" o "enriquecimiento de cabeceras", cuando navega por la red móvil Movistar con el APN teléfonica.es - Sólo se puede evidenciar una racionalización de su uso desde 2015. - Incumplimiento de obligaciones de información (uso generalizado) o de establecimiento de un procedimiento de rechazo del tratamiento de datos.*	SEPT. 2016

***: El enriquecimiento de cabeceras es una funcionalidad utilizada únicamente en el protocolo HTTP que permite añadir meta-información a las peticiones acceso a una página web concreta que se progresa desde el terminal del cliente hasta el servidor final.*

En un entorno con cada vez más sanciones…

Y que no sólo ocurren en España, y que pueden deberse a ataques externos (no se trata únicamente de un incumplimiento “voluntario” de la normativa de RGPD)**:**

CAUSAS

NOV. 2018

Multa de más de 1 millón de euros a Uber por una filtración de datos en el ciberataque de 2016

*- **El ataque hizo que los datos de 57 millones de usuarios quedaran expuestos, según reguladores de Reino Unido y Países Bajos***
- Uno de los fallos de seguridad afectó a 174.000 personas en Países Bajos, de los que se filtraron nombres, direcciones de e-mail y teléfonos de clientes y conductores.
*- Además, **no protegió eficazmente** la información personal de sus clientes durante el ciberataque, que afectó a 2,7 millones de ciudadanos británicos. Sin embargo, **los clientes y conductores no fueron advertidos sobre el incidente durante más de un año** y, en su lugar, Uber pagó a los piratas informáticos 100.000 dólares a cambio de la destrucción de los registros descargados durante el ataque.*

Esto supone obviamente un incremento de los riesgos de las empresas, existiendo más miedo que visión de oportunidad por las compañías, si bien existen ya visiones más estratégicas en la industria:

Bankia

*“Los clientes también necesitan que **desde las entidades financieras se les garantice el derecho a la privacidad y la seguridad de sus datos personales”. “**Esto es lo que defendemos desde Bankia: **la ética digital”.***
***“Ni las personas ni las empresas van a utilizar una tecnología en la que no puedan confiar”.** Las entidades vencedoras serán las que “den una **respuesta de alta calidad** en las relaciones virtuales de sus clientes, **impulsando una ética digital que proteja la privacidad de los datos**, y al mismo tiempo acomoden la red de distribución tradicional para que no sea una desventaja sino un complemento en la multicanalidad y una fuente de ventajas **competitivas**”.*

Jose Ignacio Goirigolzarri, Presidente de Bankia, 5º Congreso Nacional de la Asociación para el Progreso de la Dirección (APD), Noviembre 2018

KEEP CODING

En un entorno con cada vez más sanciones…

Existen casos recientes que demuestran que “**no todo sirve**”… El caso de uso de la Liga de micrófono y la geolocalización de los móviles ajenos para detectar emisiones piratas en los bares.

Inclusión de este uso de micrófono en Condiciones Legales

+

Autorización de los usuarios / Consentimiento (en 2 ocasiones)

+

Uso sin perjuicio de sus usuarios y para evitar “fraude” (grave perjuicio a los equipos)

+

Utilizado como primer filtro y no como tratamiento automático (antes de realizar la denuncia, la Liga comprobaba cada caso)

+

Uso no masivo de los datos (uso del 0,75% de la información obtenida, “descartando” el 99,25% restante, según La Liga)

=

JUNIO 2019

Sanción de 250.000 € a la liga por uso no permitido de micrófono y la geolocalización de los móviles ajenos para detectar emisiones piratas en los bares.

Fuente: Denuncia de un usuario en Twitter: Jorge Morell, que provocó que se iniciase la investigación de oficio por la AEPD.

En un entorno con cada vez más sanciones…

Con un año y medio en vigor, ya hay ejemplos de sanciones por el nuevo RGPD tanto en Entidades grandes como pequeñas, mostrando que el supervisor no vigila únicamente las grandes compañías, y que actúa de forma ágil ante denuncias o indicios de incumplimiento.

Artículo 12 RGPD	Remisión de información sin mención de la política de privacidad/ tratamiento de datos
Se apercibe a la empresa XXX por infracción del artículo 12 RGPD, por tener instalado un sistema de cámaras en la vía pública y no disponer del preceptivo distintivo informativo en zona visible en su establecimiento hostelero, indicando el responsable ante el que poder ejecutar los derechos en el ámbito de protección de datos. No se le impone ninguna condena económica, pero se obliga a la empresa a colocar cartel informativo, indicando el responsable del mismo, en zona visible, y disponer de formulario (s) en el establecimiento adaptado a la Legislación vigente y a disposición de cualquier usuario del establecimiento hostelero.	

Artículo 13 RGPD	Remisión de información sin mención de la política de privacidad/ tratamiento de datos
El Reclamante se suscribió a una página web y demanda que le remitieron un correo para manifestarle que se había suscrito correctamente pero no aparecía información alguna sobre política de privacidad ni del modo como van a ser tratados sus datos. Se impone una sanción de apercibimiento a la empresa por la infracción del artículo 13 RGPD.	

Artículo 17 RGPD	Mantener imagen de un empleado que se dio de baja de la empresa
Se apercibe a la empresa XXX, porque la imagen del reclamante continúa a fecha de la denuncia, vinculada con las páginas web de la citada empresa, así como en los principales buscadores de la red, pese a que ya no trabaja en la empresa desde hace dos años.	

Artículo 21 RGPD	Envío de correos estando en la Lista Robinson
Se apercibe a la empresa XXX., debido a que enviaba correos electrónicos no deseados al reclamante a pesar de encontrarse dado de alta en la Lista Robinson y no haber tenido relación con la citada empresa ni autorizado a que le remitieran publicidad alguna.	

Artículo 22.2 LOPDGDD	Cámaras con orientación a la vía pública
Se apercibe al denunciado por la existencia de tres cámaras con orientación hacia la vía pública, sin ninguna causa justificada.	

En un entorno con cada vez más sanciones…

(Cont.)

Artículo 5.1 LOPDGDD	**Uso de correos electrónicos de un cliente, que el propio cliente no había facilitado**

Se impone a la empresa XXX una sanción de 60.000 €. La reclamante solicitó un microcrédito de 300 euros, a la entidad XXX y traspasó la deuda a la entidad de recobro XXXX. La reclamante recibía correos electrónicos de la empresa XXX, reclamando la deuda relativa al préstamo solicitado; pero las direcciones de correo electrónico usadas era, aparte de la aportadas por la reclamante al solicitar el crédito también la dirección de correo electrónico institucional del lugar del trabajo de la reclamante. Sin embargo, denuncia que en ningún momento facilitó esta última dirección.

Artículo 5.1 c) RGPD	**Publicación de datos personales de empleados de instituciones protegidas**

Se impone una sanción de apercibimiento a la Secretaría General de Instituciones penitenciarias. La reclamante presentó una solicitud para una oposición del Cuerpo Superior de Técnicos en Instituciones Penitenciarias y en la publicación del BOE figura un listado en el que consta nombre y apellidos, DNI y la edad a través de la fecha de nacimiento. Añade que, en el buscador de GOOGLE, tecleando su nombre sale la remisión a sus datos en el BOE de dicha convocatoria.

Artículo 5.1 f) RGPD	**Envío de datos de compras a un tercero mostrando sus datos personales**

Se impone una sanción de 50.000 € la empresa de telefonía XXX. El reclamante alega que el reclamado ha remitido un SMS a un tercero en el que figura un enlace que conduce a un "Resumen de Compra" de la reclamante, visualizándose sus datos.

Artículo 6 RGPD	**Inclusión indebida en el registro de morosidad**

- Se impone a la empresa XXX una multa de 60.000€. La reclamante alega que se ha hecho un uso inadecuado de sus datos personales, no comprobando su identidad e incluyéndola en el fichero de solvencia patrimonial Asnef. La empresa no acredita la legitimación para el tratamiento de los datos de la reclamante, ya que el contrato no aparece firmado y ha sido negada su formalización.
- Se apercibe a la empresa de telefonía XXX puesto que la reclamante recibe un sms exigiéndole una factura por valor de 54,94. Descubriendo la existencia de una tercera línea añadida a su contrato sin su consentimiento. La titularidad de dichas líneas ha sido modificada sin su consentimiento, de manera que, los datos personales y domiciliación bancaria que aparecen en la base de datos de la empresa no corresponden a los de la reclamante, sino a un tercero que desconoce.

Artículo 6.1. LOPDGDD	**Inclusión indebida en el registro de morosidad**

Se impone a la Clínica XXX una sanción de apercibimiento. La cláusula de envío de información comercial por parte de la clínica reclamada establece que para no recibir publicidad hay que marcar una casilla lo cual se considera contrario a la normativa de protección de datos que establece que para la remisión de publicidad se necesita un acto afirmativo, y no uno negativo.

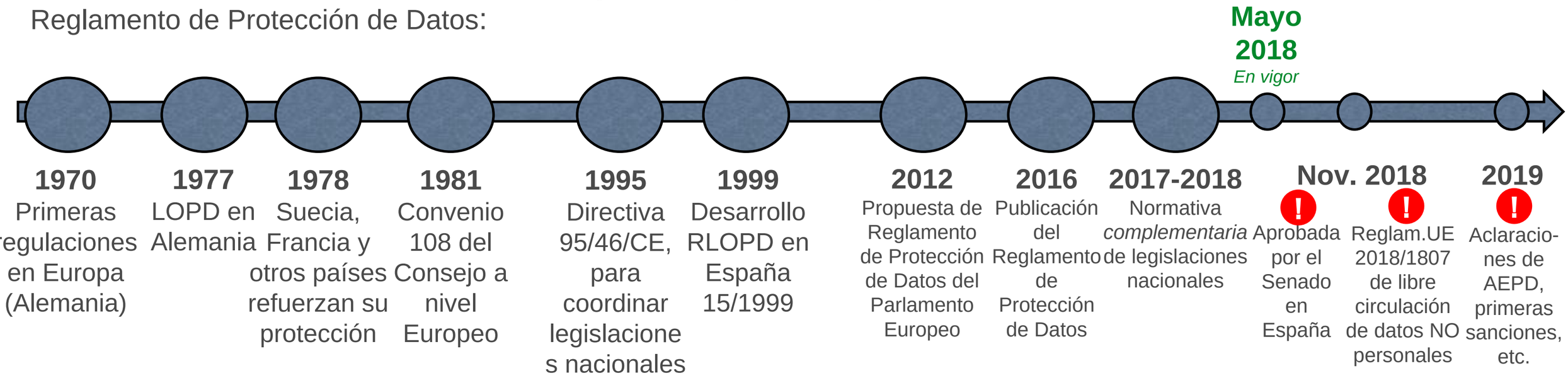
En un entorno con cada vez más sanciones…

Nivel de Criticidad	Sanciones LOPD (vigente hasta 2018)	Sanciones nuevo RGPD (a partir de 25 de Mayo de 2018)
Leves *Por ejemplo:* *- No solicitar la inscripción del fichero en la Agencia Española de Protección de Datos (AEDP).* *- Recopilar datos personales sin informar previamente*	Hasta 60.000 €	De hasta 10.000.000 € ó 2% del volumen de negocio del año anterior. Hasta 20.000.000 € ó 4% del volumen de negocio del año anterior. (RGPD – Artículo 83)
Graves *Por ejemplo:* *- Utilizar los ficheros con distinta finalidad con la se crearon.* *- No tener el consentimiento del interesado para recabar sus datos personales*	Entre 60.000 y 300.000 €	
Muy Graves *Por ejemplo:* *Recabar datos especialmente protegidos sin la autorización del afectado.* *No atender u obstaculizar de forma sistemática las solicitudes de cancelación o rectificación.*	Entre 300.000 y 600.000 €	

La AEPD tiene la posibilidad de realizar apercibimientos sin sanción con carácter discrecional, de forma excepcional, en función de los aspectos que se detecten en sus revisiones..

Reglamento GDPR

En las últimas décadas se ha fortalecido la regulación específica de protección de datos hasta terminar en el actual Reglamento de Protección de Datos:



Estas regulaciones han permitido **mejorar el marco de actuación a nivel europeo, y en los últimos años adaptar una realidad normativa a un entorno muy diferente al que existía cuando se escribieron por primera vez estas normas**. También es relevante que el ámbito territorial se extiende a empresas fuera de la UE que realizan sus actuaciones en la UE, aunque **no consigue reducir de forma completa los problemas de coordinación con otros países con otras regulaciones (Estados Unidos, Sudámerica…), y que la norma sigue "ajustándose" incluso después de su entrada en vigor "oficial" en Mayo de 2018.**

Reglamento GDPR – Introducción / Conceptos

En mayo de 2016 se publicó el nuevo Reglamento Europeo de Protección de Datos Personales, que supone el mayor hito legislativo en materia de privacidad y protección de datos personales en los últimos años:

- Datos personales
- Derechos ARCO
- Consentimiento
- Niveles de criticidad
- Encargado del tratamiento
- Importador / Exportador de Datos Personales
- Ficheros de titularidad privada / pública
- Responsable del fichero o del tratamiento
- Transferencia internacional de Datos
- Responsable de Seguridad

En estos ejercicios las Entidades se enfrentan al problema de que puede resultar sencillo realizar asignación de controles, responsables, encargados, etc. para un dato concreto, pero sin una sistemática clara resultará imposible realizarlo para todos los datos de la organización.

Reglamento GDPR – Introducción / Conceptos

Se introducen algunas definiciones de partida necesarias para analizar el impacto en la protección de los datos:

Datos personales	Toda información sobre una persona física **identificable** («el interesado»), esto es, cuya identidad pueda determinarse, directa o indirectamente, mediante un identificador, como por ejemplo un nombre, un número de identificación, 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.
Derechos ARCO	Derechos de **acceso, rectificación, cancelación y oposición** que garantizan a las personas el poder de control sobre sus datos personales.
Consentimiento	Toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen
Niveles de criticidad	Niveles asignados que suponen mayor o menor exigencia en cuanto a medidas de seguridad exigibles a los ficheros y tratamientos de datos personales: Existen los niveles **BÁSICO, MEDIO y ALTO**. Esta clasificación se realiza atendiendo a la naturaleza de la información tratada, en relación con la menor o mayor necesidad de garantizar la confidencialidad y la integridad de la información.
Datos especialmente protegidos	DATOS ESPECIALMENTE PROTEGIDOS Advertir al interesado de su derecho a no prestar su consentimiento en el tratamiento de estos datos. Se necesita consentimiento expreso y por escrito del interesado para el tratamiento de datos que revelen ideología, afiliación sindical, religión y creencias. Se necesita consentimiento expreso o que lo disponga una ley para recabar, tratar o ceder datos relativos a origen racial, salud o vida sexual. No se permite crear ficheros con la única finalidad de almacenar datos de carácter personal, que revelen ideología, afiliación sindical, religión, origen racial, salud o vida sexual. Se podrán tratar, no obstante, los datos anteriores, si resulta necesario para el diagnóstico médico o la asistencia sanitaria..

Reglamento GDPR (2016)

En mayo de 2016 se publicó el nuevo Reglamento Europeo de Protección de Datos Personales, que supone el mayor hito legislativo en materia de privacidad y protección de datos personales en los últimos años:

Reglamento
1 Disposiciones generales
2 Principios
3 Derechos del interesado
4 Responsable del tratamiento y encargado del tratamiento
5 Transferencias de datos personales a terceros países u organizaciones internacionales
6 Autoridades de control independientes
7 Cooperación y coherencia
8 Recursos, responsabilidad y sanciones
9 Disposiciones relativas a situaciones específicas de tratamiento
10 Actos delegados y actos de ejecución
11 Disposiciones finales

Principales Impactos

- Cambios organizativos en la vigilancia de los datos a nivel europeo.
- Refuerzo de las obligaciones de información a los "interesados"
- Creación de la figura del Delegado de Protección de Datos dentro de la Entidad.
- Régimen de sanciones económicas derivadas de la vulneración de derechos.
- Necesidad de establecer los usos / fines de la información.
- Regular y evitar la recogida indiscriminada de datos.
- Responsabilidad proactiva de las Entidades.

*En conclusión, un nuevo **MARCO de actuación** en la protección de datos de carácter personal, que supone no sólo cambios en las políticas y procedimientos de las empresas reguladas, sino **cambios reales relevantes en los sistemas de estas compañías**.*

Reglamento GDPR (2016)

Entre los cambios más relevantes, destacar la figura que debe tener **un control global** en las empresas más relevantes:

¿Quién debe disponer de un DPO?

- ✓Las Administraciones Públicas (autoridades y organismos, excepto Tribunales)
- ✓Empresas y otras entidades cuya actividad principal consista en el tratamiento masivo de datos personales que, por su naturaleza, alcance o fines, requieran una observación habitual, sistemática y a gran escala de sus titulares.
- ✓Empresas y otras entidades cuya actividad principal consista en el tratamiento a gran escala de categorías de datos personales especialmente protegidas (artículo 9) y de datos relativos a condenas e infracciones penales (artículo 10).

Funciones del Data Protection Officer

- ✓**Informar y asesorar al responsable o al encargado del tratamiento** y a los empleados que se ocupen del tratamiento de las obligaciones que tienen.
- ✓**Supervisar el cumplimiento** de lo dispuesto en:
  - el presente Reglamento.
  - otras disposiciones de protección de datos de la Unión o de los Estados miembros.
  - políticas del responsable o del encargado del tratamiento en materia de protección de datos personales.
- ✓**Ofrecer el asesoramiento que se le solicite** acerca de la evaluación de impacto.
- ✓**Cooperar con la autoridad** de control.
- ✓**Actuar como punto de contacto de la autoridad** de control para cuestiones relativas al tratamiento.
- ✓**Dar respuestas** a todos los **requerimientos de información** realizados por los **titulares de los datos personales** para solventar cualquier duda al respecto del tratamiento de sus datos.

LOPD en España

Al margen de las modificaciones que surgen por GDRP (2016) y que se aplicarán a la LOPD en España, la mayoría de los preceptos ya aplicanban en la LOPD de 2007, ya aplicables en la protección de datos en España:

RLOPD

- Título I: Disposiciones Generales
- Título II: Principios
- Título III: Derechos
- Título IV: Disposiciones
- Título V: Obligaciones previas al tratamiento de datos
- Título VI: Transferencias de datos internacionales
- Título VII: Códigos tipo
- Título VIII: Medidas de seguridad en el tratamiento de datos personales
- Título IX: Procedimientos tramitados por la AEPD
- Otras disposiciones…

Título II: Principios

- Calidad de los datos (Artículo 4)
- Derecho de la información en la recogida de datos (Artículo 5)
- Consentimiento del afectado (Artículo 6)
- Datos especialmente protegidos (Artículo 7)
- Datos relativos a la salud (Artículo 8)
- Seguridad de los datos (Artículo 9)
- Deber de secreto (Artículo 10)
- Comunicación de los datos (Artículo 11)
- Acceso a los datos por cuenta de terceros (Articulo 12)

Título III: Derechos

- Derecho de acceso (Artículo 27)
- Derecho de rectificación y cancelación (Artículo 31)
- Derecho de oposición (Artículo 34)

LOPD en España – Ejemplo de Medidas de Seguridad

Los artículos de medidas de seguridad del Real Decreto 1720/2007 permiten concretar **CÓMO** cumplir los “derechos y principios”:

FICHEROS AUTOMATIZADOS:

1. Medidas de seguridad de **NIVEL BÁSICO**

- √ **Artículo 89 Funciones y obligcs. del personal**
- √ **Artículo 90 Registro de incidencias**
- √ **Artículo 91 Control de acceso**
- √ **Artículo 92 Gestión de soportes y documentos**
- √ **Artículo 93 Identificación y autenticación**
- √ **Artículo 94 Copias de respaldo y recuperación**

2. Medidas de seguridad de **NIVEL MEDIO**

- √ **Artículo 95 Responsable de seguridad**
- √ **Artículo 96 Auditoría**
- √ **Artículo 97 Gestión de soportes y documentos**
- √ **Artículo 98 Identificación y autenticación**
- √ **Artículo 99 Control de acceso físico**
- √ **Artículo 100 Registro de incidencias**

3. Medidas de seguridad de **NIVEL ALTO**

- √ **Artículo 101 Gestión y distribución de soportes**
- √ **Artículo 102 Copias de respaldo y recuperación**
- √ **Artículo 103 Registro de accesos**
- √ **Artículo 104 Telecomunicaciones**

FICHEROS NO AUTOMATIZADOS:

1. Medidas de seguridad de NIVEL BÁSICO

- √ **Artículo 105 Obligaciones comunes**
- √ **Artículo 106 Criterios de archivo**
- √ **Artículo 107 Dispositivos de almacenamiento**
- √ **Artículo 108 Custodia de los soportes**

2. Medidas de seguridad de NIVEL MEDIO

- √ **Artículo 109 Responsable de seguridad**
- √ **Artículo 110 Auditoría**

3. Medidas de seguridad de NIVEL ALTO

- √ **Artículo 111 Almacenamiento de la información**
- √ **Artículo 112 Copia o reproducción**
- √ **Artículo 113 Acceso a la documentación**
- √ **Artículo 114 Traslado de documentación**

Los controles más exhaustivos se dan sobre procesos automatizados, fortaleciéndose en el resto los procedimientos de gobierno

KEEP CODING

LOPD en España – Ejemplo de Medidas de Seguridad

Estas medidas se seguridad se implementan partiendo de guías y procedimientos de AEPD:

El presente Documento y sus Anexos, redactados en cumplimiento de lo dispuesto en el RLOPD recogen las medidas de índole técnica y organizativa necesarias para garantizar la protección, confidencialidad, integridad y disponibilidad de los recursos afectados por lo dispuesto en el citado Reglamento y en la LOPD. El contenido es el siguiente:

- Ámbito de aplicación del documento.

- Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar los niveles de seguridad exigidos en este documento.

- Información y obligaciones del personal.

- Procedimientos de notificación, gestión y respuestas ante las incidencias.

- Procedimientos de revisión.

ANEXO I. Descripción de ficheros.

ANEXO II. Nombramientos.

ANEXO III. Autorizaciones de salida o recuperación de datos.

ANEXO IV. Delegación de autorizaciones.

ANEXO V. Inventario de soportes.

ANEXO VI. Registro de Incidencias.

ANEXO VII. Encargados de tratamiento

ANEXO VIII. Registro de entrada y salida de soportes.

ANEXO IX. Medidas alternativas

RGPD en España – Ejemplo de Guía de Privacidad desde el Diseño

Los preceptos del nuevo RGPD se documentan en guías impulsadas por la AEPD para facilitar que las compañías adapten sus procedimientos y adopten mejores prácticas:

En el documento figuran los **principios fundacionales de la privacidad desde el diseño**: 1. Proactivo, no reactivo; preventivo, no correctivo; 2. La privacidad como configuración predeterminada; 3. Privacidad incorporada en la fase de diseño; 4. Funcionalidad total: pensamiento “todos ganan” ; 5. Aseguramiento de la privacidad en todo el ciclo de vida ; 6. Visibilidad y transparencia y 7. Respeto por la privacidad de los usuarios: mantener un enfoque centrado en el usuario

La guía también profundiza en la **ingeniería de la privacidad** (privacy engineering) como un proceso sistemático y dirigido por el enfoque al riesgo con objetivo de **traducir en términos prácticos y operativos los principios de la privacidad desde el diseño** (PbD) dentro del ciclo de vida de los sistemas encargados del tratamiento de datos personales, y otras estrategias de PbD.

Para dar cobertura a estos posibles riesgos han de incluirse en el **esquema de análisis 3 nuevos objetivos de protección**, específicos de la privacidad, y cuya garantía se convierte en salvaguarda de los principios de tratamiento del RGPD:

- **Desvinculación (*Unlinkability*)**: persigue que el procesamiento de la información se realice de modo que los datos personales de un dominio de tratamiento no puedan vincularse con datos personales de otro dominio diferente, o que el establecimiento de dicha vinculación suponga un esfuerzo desproporcionado.
- **Transparencia (*Transparency*)**: busca clarificar el tratamiento de los datos para que la recogida, procesamiento y uso de la información pueda ser comprendido y reproducido por cualquiera de las partes implicadas y en cualquier momento del tratamiento.
- **Control (*Intervenability*):** garantiza la posibilidad de que las partes involucradas en el tratamiento de los datos personales y, principalmente, los sujetos cuyos datos son tratados, pueden intervenir en el tratamiento cuando sea necesario para aplicar medidas correctivas al procesamiento de la información.

En el documento se describen las **ocho estrategias de diseño de la privacidad más comunes** que se conocen como ‘minimizar’, ‘ocultar’, ‘separar’, ‘abstraer’, ‘informar’, ‘controlar’, ‘cumplir’ y ‘demostrar’.

NOV. 2018

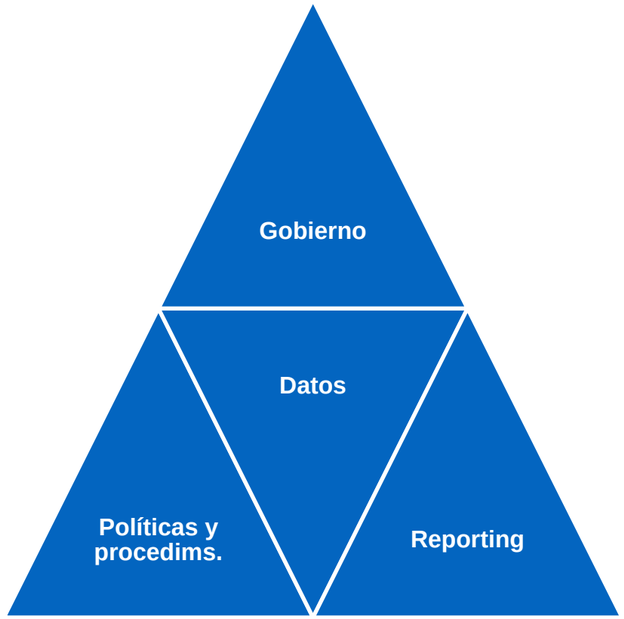
Reglamento - Protección de datos NO personales

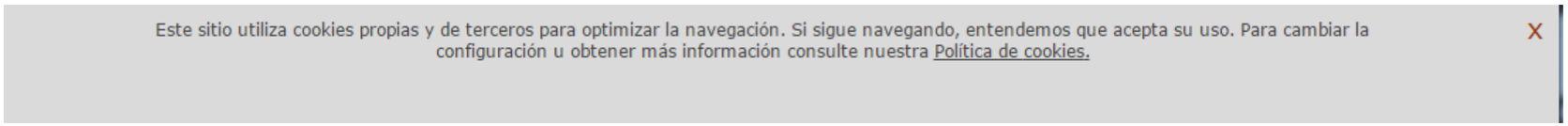
Se introducen algunas definiciones para tener en cuenta medidas adicionales incluso con datos NO personales, a partir del Reglamento publicado en Noviembre de 2018:

Datos NO personales	Datos que no sean datos personales tal como se definen en el artículo 4, punto 1, del Reglamento (UE) 2016/679. En conclusión, definición contraria a la del RGPD.
Objetivo	Garantizar la libre circulación en la Unión de datos que no tengan carácter personal mediante el establecimiento de normas relativas a los requisitos de localización de datos, la disponibilidad de los datos para las autoridades competentes y la portabilidad de datos para los usuarios profesionales con la finalidad de regular la digitalización de la economía y resolver los problemas jurídicos planteados por el rápido desarrollo de la economía de datos y las tecnologías emergentes como la inteligencia artificial. **Los requisitos de localización de datos** constituyen un claro obstáculo a la libre prestación de servicios de tratamiento de datos en la Unión y al mercado interior. Como tales, **deben ser prohibidos** a menos que estén justificados por motivos de **seguridad pública**,
A quién aplica	Aplica a los servicios que se presten como un servicio a **usuarios que residan o tengan un establecimiento en la Unión Europea o se efectúen por una persona física o jurídica** que resida o tenga un establecimiento **en la Unión** para sus propias necesidades. En cambio, no se aplicará a las actividades que no entren en el ámbito de aplicación del Derecho de la Unión.
Códigos de Conducta	La Comisión fomentará y facilitará la elaboración de **códigos de conducta (autorreguladores)** a escala de la Unión, con el fin de contribuir a una economía de datos competitiva, basada en los principios de transparencia e interoperabilidad. **La Comisión alentará a los proveedores de servicios a completar el desarrollo de los códigos de conducta a más tardar el 29 de noviembre de 2019 y a aplicarlos efectivamente a más tardar el 29 de mayo de 2020. Y a más tardar el 29 de mayo de 2019, la Comisión publicará orientaciones informativas sobre la interacción de este reglamento y del Reglamento 2016/679.**
Entrada en vigor	La fecha de aplicación de este Reglamento, será seis meses después de su publicación (**MAYO 2019**), con las consideraciones previas realizadas en el punto anterior del impulso de **la aplicación de los Códigos de Conducta antes del 29 de Mayo de 2020**.

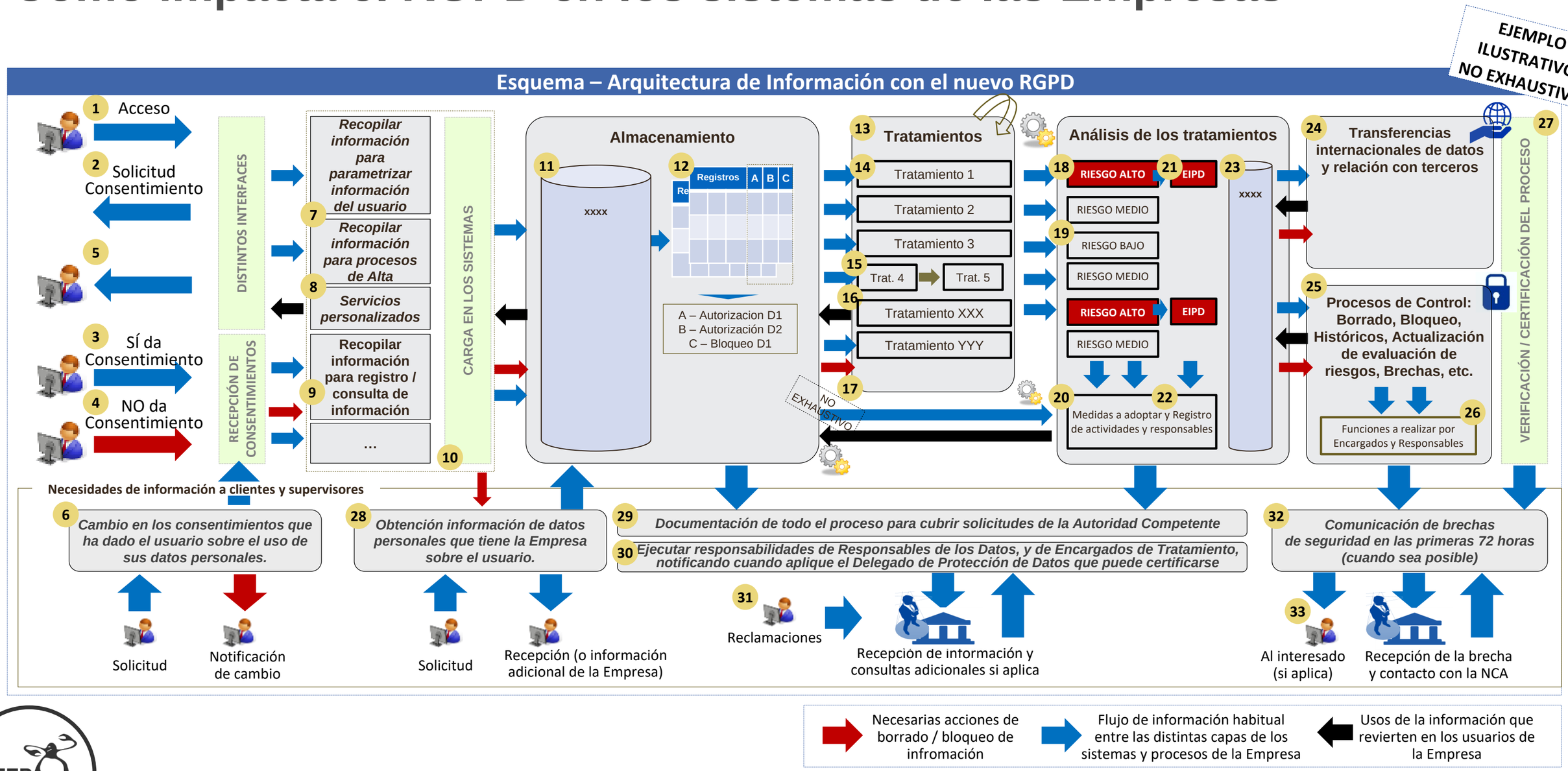
Protección de datos: Enfoque transversal

Cumplir con la Ley de Protección de Datos es cada vez más un reto transversal de las organizaciones, y no únicamente un inventario de disclaimers legales:

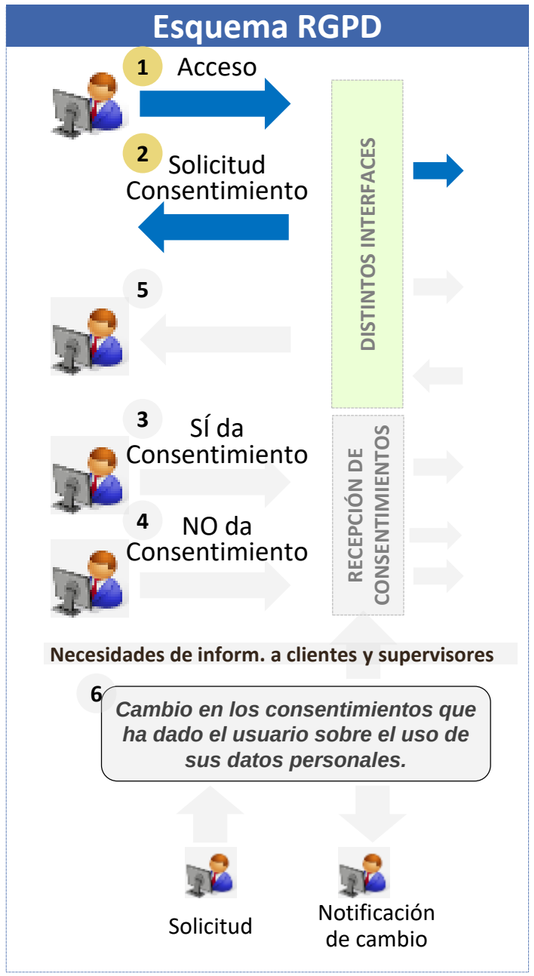




Cómo impacta el RGPD en los sistemas de las Empresas



Cómo impacta el RGPD en los sistemas de las Empresas



1 Los usuarios acceden a los sistemas de las Entidades fácilmente, casi sin darse cuenta, entre otros motivos porque hasta ahora muchas compañías aceptaban "por omisión" del usuario su consentimiento a tratar los datos.

Para cumplir la obligación de notificación, las Compañías cuentan con una **Política de Privacidad** en la que **informan del tratamiento de los datos**, recogiendo tanto las obligaciones que se impone la Empresa, como los derechos de los interesados, debiendo adecuar el resto de comunicaciones a estos principios (comunicaciones "menos farragosas"):

- *"El principio de transparencia exige que toda información dirigida al público o al interesado sea **concisa, fácilmente accesible y fácil de entender**, y que se utilice un **lenguaje claro y sencillo**, y, además, en su caso, **se visualice**. Esta información podría facilitarse en forma electrónica, por ejemplo, cuando esté dirigida al público, mediante un sitio web." (Considerando 58 RGPD)*

La LOPD ya establecía obligaciones de información a facilitar a los interesados en el momento en que se soliciten los datos como la existencia del fichero o tratamiento, su finalidad y destinatarios, posibilidad de ejercitar derechos ARCO, el carácter obligatorio de la respuesta, y la identidad y datos de contacto del responsable del tratamiento.

Se incrementa nivel de exigencia respecto a LOPD (2007)

2 A partir de ahora, el RGPD añade requisitos adicionales en cuanto a la **necesidad de informar a las personas interesadas**, generalizando el concepto de "Tratamiento", e incorporando, detalles sobre cómo contactar al Delegado de Protección de Datos, **la base que legitima el tratamiento de los datos**, el plazo o criterios de conservación de la información, la existencia de decisiones automatizadas o perfiles, previsión de transferencias a otros países, el derecho a presentar una reclamación a las Autoridades de Control y, en el caso de que los datos no se obtengan del propio interesado, el origen de los datos y sus categorías.

Los principios que legitiman el **tratamiento de datos,** que **deben estar documentados** (para que "puedan demostrarse") son:

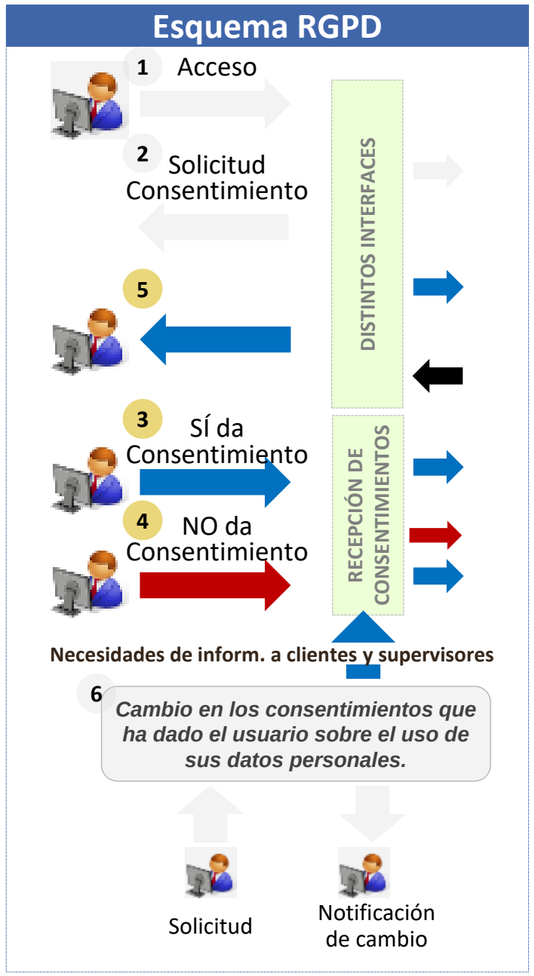
- Relación contractual, o intereses vitales del interesado u otras personas.
- Misión de interés público o "ejercicio de poderes públicos".
- Obligación legal del responsable o intereses legítimos del responsable / terceros a los que se comunican datos (i.e: una ***reclamación***).

Si no se encuentra una de estas causas es necesario, para cumplir con la "base legítima", **recabar consentimiento del usuario**.

El consentimiento debe ser "inequívoco", y **en algunos casos "expreso"**: Tratamiento de datos "sensibles", Adopción de decisiones "automatizadas" y acciones que suponen transferencias internacionales de datos.
Los **consentimientos previos siguen siendo válidos** si se cumplieron estas premisas.

Se evita de forma general el consentimiento "por omisión" que se prestaba en LOPD (2007)

Cómo impacta el RGPD en los sistemas de las Empresas



3 Los usuarios pueden dar el consentimiento ante la solicitud de la empresa, **realizando una acción específica**. Este consentimiento, no obstante, debe cumplir una serie de criterios de información y podrá cambiarse por el usuario a futuro. Para que un consentimiento se considere válido, en el caso de un menor, este se deberá realizar por un menor de al menos 16 años según el
4 RGPD europeo (si bien se permite a las Entidades nacionales permitirlo hasta 13 años).

El usuario puede **elegir si dar su consentimiento o no a los diferentes tratamientos**, no existiendo un único consentimiento para tratamientos completamente diferentes de la información. **Así, un usuario puede aprobar el uso de su información para ciertas actividades** relacionadas con el servicio contratado (por ejemplo, utilizar sus datos para adaptar la información que se le muestra en la plataforma a la que tiene acceso), pero **rechazar otros tratamientos** como que esos datos sean comunicados a terceros y puedan utilizarse para otros fines comerciales no relacionados con el servicio.

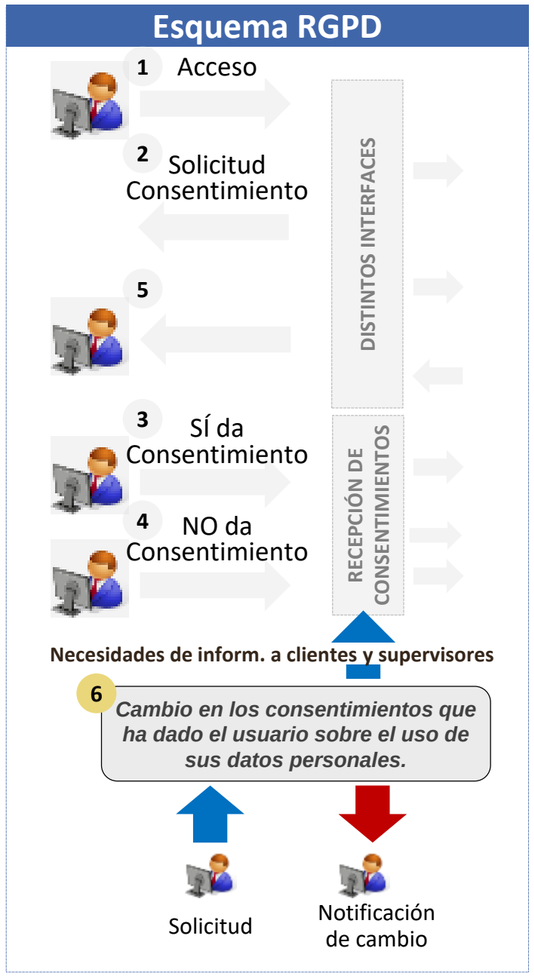
- *"Por tanto, el silencio, las **casillas ya marcadas** o la **inacción** no deben constituir consentimiento. El consentimiento debe **darse para todas las actividades de tratamiento** realizadas **con** el mismo o **los mismos fines**. Cuando el tratamiento **tenga varios fines, debe darse el consentimiento para todos ellos**. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta." (Considerando 32 RGPD).*
- Adicionalmente: *El consentimiento **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** (Considerando 42).*

Mayor granularidad de los consentimientos que en LOPD previa

5 El RGPD, cómo ya se ha comentado en el punto 2 anterior, no requiere consentimiento para alguna acciones de los usuarios. Esto **puede darse cuando el consentimiento se deduce de una acción del interesado** (por ejemplo, cuando el interesado continúa navegando en una web y acepta así que se utilicen **cookies** para **monitorizar su navegación**).

Estos consentimientos también deben guardarse en los sistemas pues suponen un tratamiento de información del usuario, pero no impiden proporcionar esta particularización del servicio al usuario hasta que el usuario realice una acción adicional de consentimiento.

Cómo impacta el RGPD en los sistemas de las Empresas



6 Los usuarios pueden cambiar su consentimiento a lo largo de la vida de la relación con la Empresa, para cumplir el RGPD que indica:

- *"El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello". (Artículo 7)*

Actualmente, muchas compañías permitían revocar este consentimiento con procedimientos engorrosos que suponían, en la práctica, que pocos clientes pudieran solicitarlo. Sin embargo, esto ya no resulta admisible, toda vez que el nuevo RGPD indica expresamente, también el artículo 7:

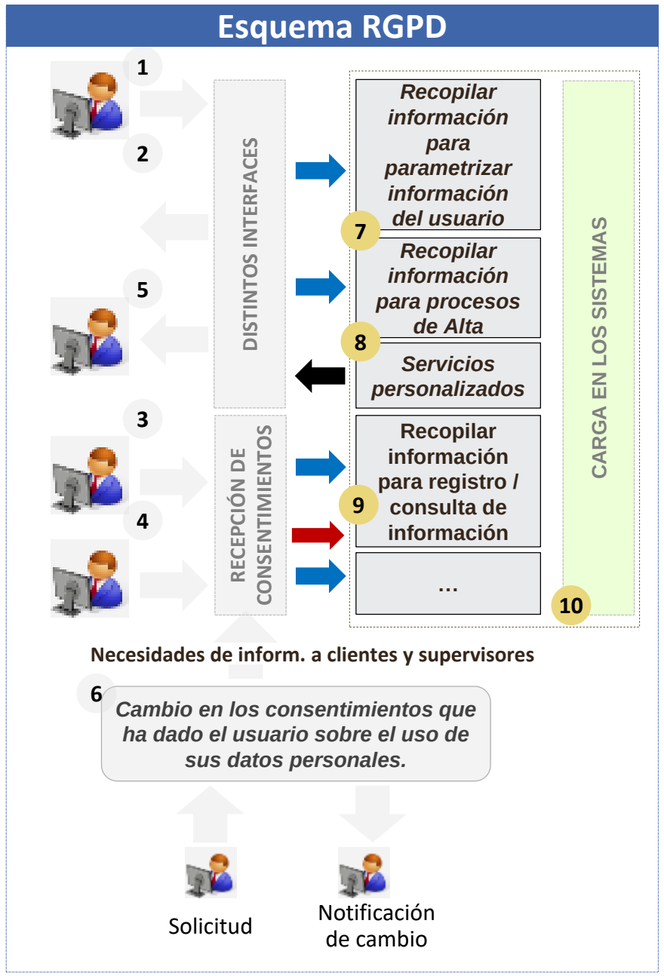
- *"Será tan fácil retirar el consentimiento como darlo". (Articulo 7)*

Para que el usuario sea consciente de este derechos, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, entre otros (…), **la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento** basado en el consentimiento previo a su retirada. (Artículo 13).

Como otros derechos, debe facilitarse de forma gratuita, salvo peticiones excesivas.

Cuando se retira el consentimiento al uso de los datos, será responsabilidad de la empresa el borrado de estos datos, o al menos su bloqueo, para que no sean utilizados, tal y como ha solicitado el interesado (salvo una causa mayor, que implique un interés legítimo del interesado como su uso ante una reclamación, u otras causas tasadas).

Cómo impacta el RGPD en los sistemas de las Empresas



7 Existirá procesos que tomarán los datos proporcionados por los interesados, ya sea a través de medios electrónicos u otros medios, que deben darse. Estos procesos deben **preservar la exactitud (y, si aplica, la actualización)** de los datos. Entre los diferentes procesos para almacenar la información, la Empresa puede completar los datos que han sido recabados del cliente con otros datos de los que disponga del usuario, completándose los proceso de alta de una relación con el cliente.

8 **Algunos de los consentimientos obtenidos permiten dar un tratamiento personalizado al cliente**, que puede redundar en una mejor experiencia del cliente. El **RGPD no trata de evitar que se presten estos servicios, sino que busca transparentar los usos** que se hacen de la información de los usuarios, así como **dar permiso al interesado para autorizarlo** o no.

9 Entre esta obtención de información, está la necesidad de incorporar en los procesos los propios consentimientos. Generalmente, se asocia el cumplimiento del RGPD a las bases de datos con información del cliente, pero el propio reglamento insiste en que afecta a la totalidad de los procesos de obtención o tratamiento de información del cliente, con el concepto de "medidas de Protección de Datos **desde el Diseño y por defecto**" o con "**medidas de seguridad**". Esto supone:

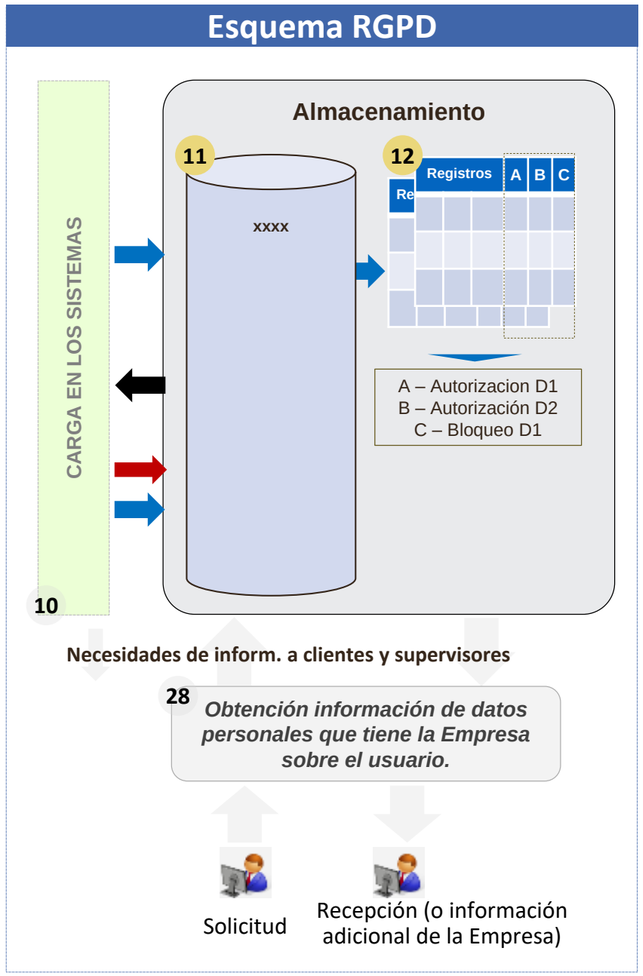
- *El responsable del tratamiento debe **adoptar políticas internas y aplicar medidas** que cumplan en particular los principios de **protección de datos desde el diseño y por defecto**. Dichas medidas podrían consistir, entre otras, en:*
  - *- **Reducir al máximo** el tratamiento de datos personales,*
  - *- **Seudonimizar lo antes posible** los datos personales,*
  - *- Dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad.*

*Ha de alentarse a los productores a que tengan en cuenta el derecho a la protección de datos **cuando desarrollan y diseñen estos productos, servicios y aplicaciones**, y que se aseguren, **con la debida atención** al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos. (Considerando 78, y artículo 25)*

Podrá utilizarse un mecanismo de certificación para acreditar su cumplimiento. (Artículo 25).

10 Una vez obtenida la información, y evaluados los consentimientos que se han proporcionado por los diferentes medios, se almacena la información en los sistemas de la Empresa.

Cómo impacta el RGPD en los sistemas de las Empresas



11 Las bases de datos informacionales cuentan con información identificada por cliente, pero el reglamento general de protección de datos obliga en la práctica a tener asociado cómo se ha obtenido el consentimiento de cada dato en los sistemas. Las organizaciones, ya sea creando sistemas "espejo" a los sistemas informacionales que guardan la información de los consentimientos, ya sea integrando la información en la propia base de datos, para facilitar cualquier tratamiento posterior de los datos, están pasando a cumplir las obligaciones del reglamento **integrando esta información como un eje adicional**.

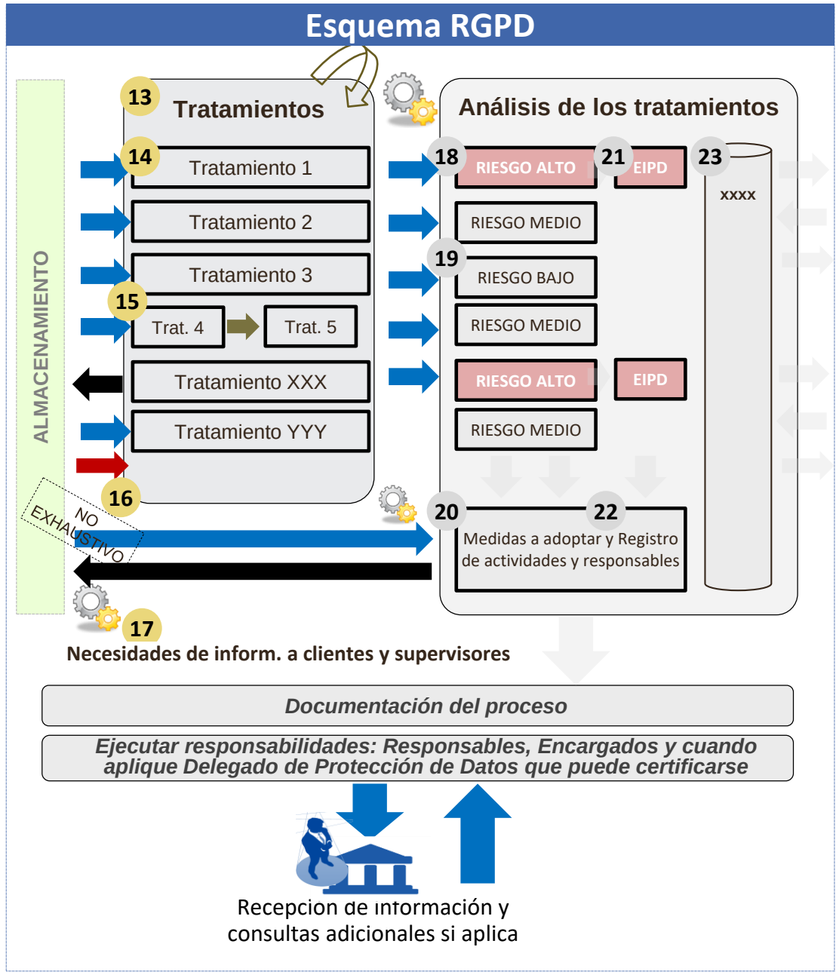
Es necesario, una vez almacenados los datos, que **cualquier proceso (o usuario libre)** que vaya a tomar esos datos pueda explotar la información teniendo en cuenta los consentimientos, **pues sino cualquier tratamiento realizado previamente o consentimiento parcial implantado no será seguido en el resto de capas** de información de la empresa:

12 La información registrada en los sistemas puede permitir:

- Que la Base de Datos no muestre ciertos datos a los usuarios cuando realicen su consulta (datos que deben mantenerse en la base de datos por otros "intereses legítimos".
- Que la Base de Datos muestre datos de forma parcial en función del proceso / usuario que los vaya a utilizar.
- Que se puedan producir borrados periódicos de los datos sin consentimiento cuando se haya cumplido el plazo / situación que habilitaba mantener los datos.
- Que se puedan propagar al resto de aplicaciones / tratamientos / terceros únicamente la información que pueda tratarse conforme al RGPD.
- …

¿Cuáles aplican en tus proyectos de extracción de datos?

Cómo impacta el RGPD en los sistemas de las Empresas



13 Una vez pasado el proceso de obtención y almacenamiento de la información de los interesados, el bloque funcional en el que más profundiza el RGPD es el de tratamiento de la información, entendiéndose el tratamiento como "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados" (Artículo 12.4).

14 **Es necesario que las Entidades conozcan los diferentes tipos de tratamiento que realizan sobre los datos personales de los clientes, pudiendo diferenciar estos tratamientos cuando el uso que se va a realizar de los datos (o la base legal en que se apoya) sea diferente**. Esto provocará problemas de granularidad en el "inventario" de los tratamientos de información que existen en la empresa, y que será necesario documentar.

15 Así, cuando existan diferentes tratamientos que tengan nivel de riesgo diferentes, aunque supongan un único entregable para la empresa, deberán identificarse y documentarse de forma diferenciada, permitiendo a los responsables / encargados adoptar las medidas que se consideren necesarias.

El responsable podrá contar con la colaboración de los encargados para atender al ejercicio de derechos de los interesados, pudiendo incluir esta colaboración en el **contrato de encargo de tratamiento**.

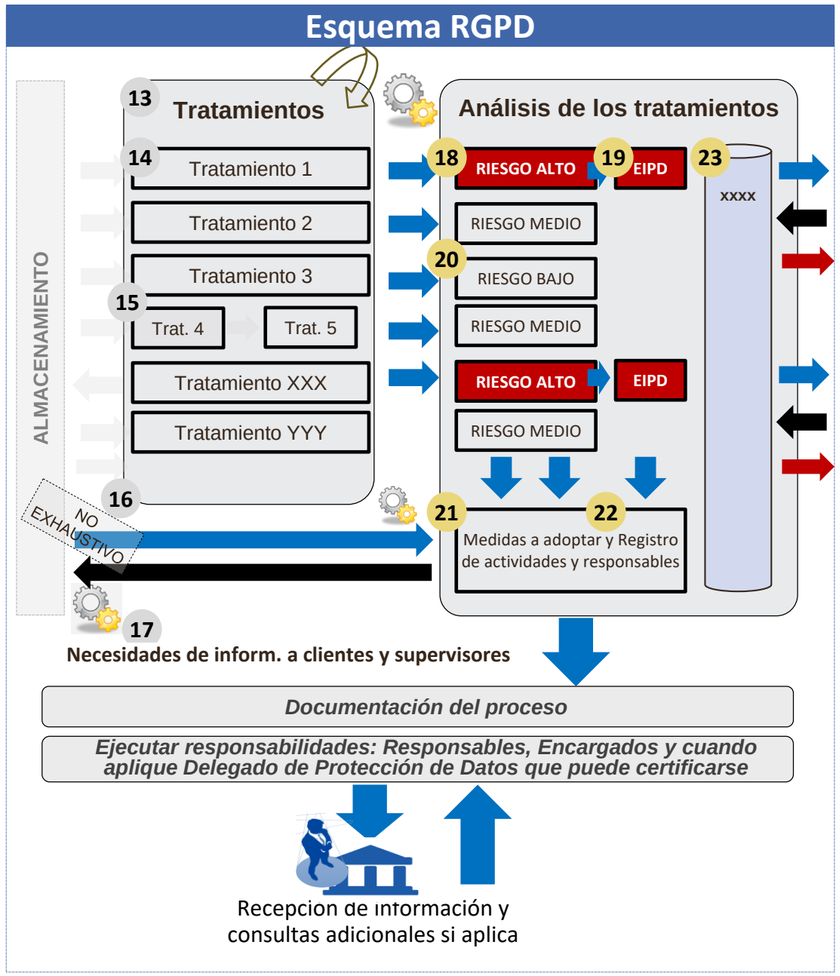
16 Al módulo de tratamientos de información deben llegar las diferentes solicitudes de los interesados, que soliciten en un momento dado que sus datos no sean tratados.

17 Del mismo modo que en otras capas informacionales, estos tratamientos deben cumplir el principio de de protección de datos **desde el diseño y por defecto**, debiendo estar los procesos existentes adaptados y tomarse en cuenta estos principios en los nuevos tratamientos que se quieran realizar.

Nuevas responsabilidades repartidas entre responsable y encargado de tratamiento, con contrato establecido

KEEP CODING

Cómo impacta el RGPD en los sistemas de las Empresas



18 Todos los responsables **deberán realizar una valoración del riesgo de los tratamientos** que realicen, a fin de poder establecer **qué medidas deben aplicar y cómo deben hacerlo**. De forma general, el reglamento tiene en cuenta la proporcionalidad en su aplicación, por lo que el análisis de riesgo se adaptará al tipo de tratamiento y a las características de las organizaciones:

- Grandes Empresas: Uso de una metodología de análisis de riesgo existente.
- Organizaciones de menor tamaño y con tratamientos poco complejos: La AEPD indica que podrá ser una "reflexión, mínimamente documentada, sobre las implicaciones de los tratamientos en los derechos y libertades de los interesados", dando respuesta a diferentes cuestiones sobre protección de datos.

19 El reglamento establece **cuando es necesario realizar una Evaluación de Impacto sobre la Protección de Datos** (EIPD) **con carácter previo** a la puesta en marcha de aquellos tratamientos que sea probable que conlleven un alto riesgo para los derechos y libertades de los interesados. Esto implica que el mandato del Reglamento no se extiende a las operaciones de tratamiento que ya estén en curso en Mayo de 2018.

El RGPD establece un **contenido mínimo** de las Evaluaciones de Impacto sobre la Protección de Datos. La AEPD ha publicado en 2018 una Guía para realizar una EIPD, proporcionando un marco de referencia (***sig. páginas***).

20 Cuando el riesgo sea **medio o bajo**, la empresa **no tendrá la obligación de realizar una "Evaluación de impacto de protección de datos"** detallada, para poder priorizar aquellos aspectos que sí tengan riesgo alto. Esto no significa que las Entidades no documenten estas actividades, y deban plantear igualmente medidas de seguridad que eviten cualquier problema en estos tratamientos, ya sean:

21 - Previas a la evaluación de impacto, o

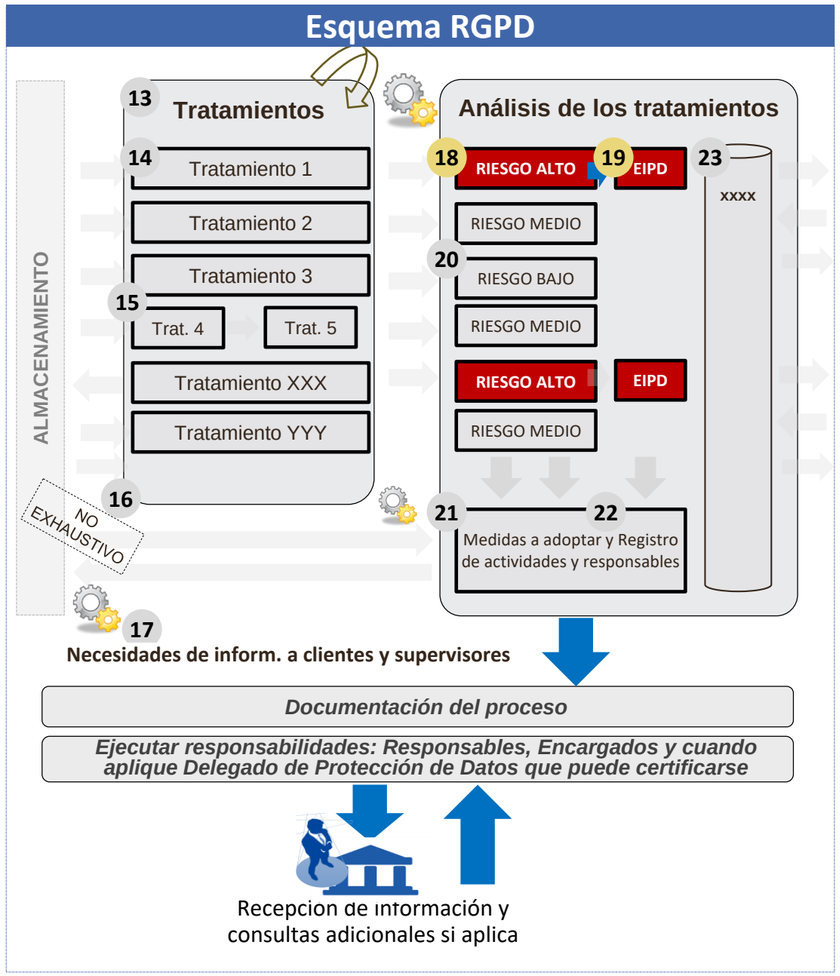
22 - Posteriores a la evaluación de impacto y necesarias para reducir el riesgo residual de un EIPD de riesgo alto.

23 El registro de actividades de tratamiento **no aplicará** en organizaciones con **menos de 250 trabajadores**, **salvo que** el tratamiento **presente riesgo** para los derechos y libertades de los interesados, **no sea ocasional o incluya categorías especiales de datos** o datos relativos a **condenas e infracciones penales**.

Si los datos tratados se almacenan en otras bases de datos, estas bases de datos deben estar protegidas y tener la posibilidad de añadir /eliminar datos de clientes ante solicitudes de los clientes.

KEEP CODING

Cómo impacta el RGPD en los sistemas de las Empresas



19 Existen algunas casuísticas que **ya se consideran de riesgo alto por defecto**:

- Elaboración de perfiles sobre cuya base se estén tomando o puedan tomarse decisiones relevantes para los interesados.
- Tratamiento a gran escala de datos sensibles.
- Observación sistemática a gran escala de una zona de acceso público

La AEPD puede completar otros casos cuando considere que tienen riesgo alto, al margen del propio análisis que tiene que realizar las Entidades de los procesos que considera que pueden tener un riesgo alto por el análisis y tratamiento de los datos realizados.

Así, el propio grupo de trabajo del artículo 29 ha introducido más criterios adicionales en el documento WP248 de Directrices sobre las Evaluaciones de Impacto en la Protección de Datos que podrían indicar, si se cumplen, que los procesos **pudieran ser de riesgo alto**:

- Uso innovador: Actividades de tratamiento realizadas mediante el uso de tecnología innovadora que pueda implicar nuevas formas de recopilación y uso de datos, posiblemente con un alto riesgo para los derechos y las libertades de las personas. Por ejemplo, la combinación del uso de la huella dactilar y el reconocimiento facial para mejorar el control del acceso físico, etc.
- Cuando el procesamiento en sí mismo “impide que los interesados ejerzan un derecho o utilicen un servicio”.
- Tratamientos sujetos a un código de conducta que lo requiere: Si a los tratamientos evaluados se les aplica un código de conducta que exige su cumplimiento también debe ser objeto de la evaluación.
- Evaluación o scoring.
- Datos relativos a personas vulnerables.

EJEMPLO ILUSTRATIVO

Las actividades de tratamiento donde se puede aplicar el enfoque de gestión de
considerando que han sido analizadas previamente mediante el análisis de la nece
una EIPD, se situarán siempre en un nivel de riesgo no elevado, tal y como se indica a conti

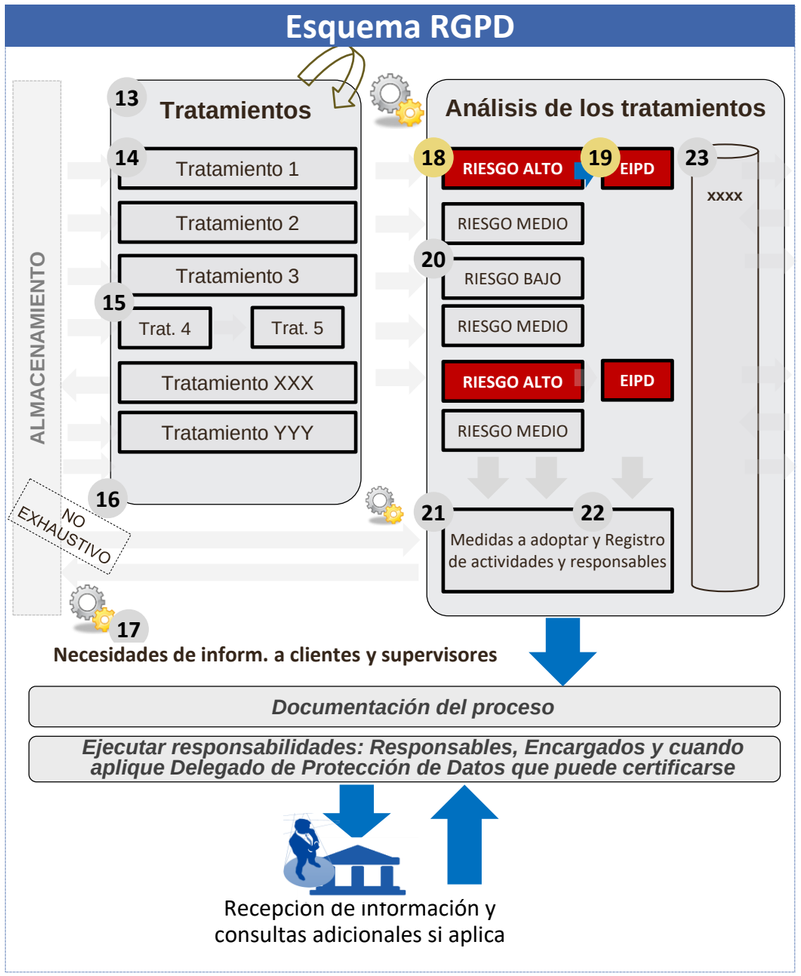
Probabilidad					
	Máxima 4	4	8	12	16
	Significativa 3	3	6	9	12
	Limitada 2	2	4	6	8
	Despreciable 1	1	2	3	4
		Despreciable · 1	Limitada · 2	Significativa · 3	Máxima · 4

Bajo
Medio
Alto
Muy Alto

IMPACTO

Cómo impacta el RGPD en los sistemas de las Empresas

ACTUALIZACIÓN AEPD – MAYO 2019



19

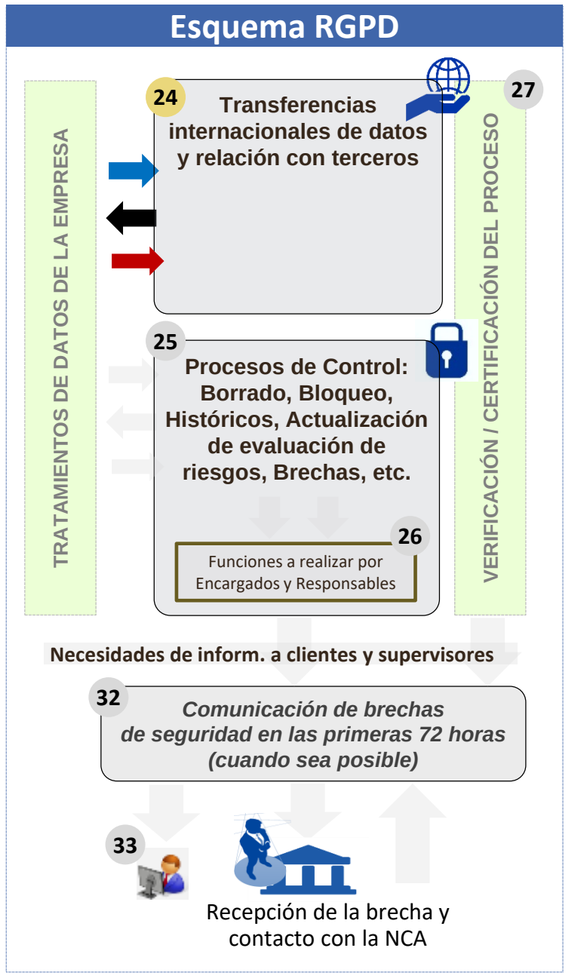
La AEPD ha **concretado** los criterios a tener en cuenta, siendo en cualquier caso necesario que las empresas que presten servicios en varios países tengan en cuenta los reglamentos y guías más "restrictivos" de todas las agencias que les supervisen. Se resumen a continuación (además, la AEPD señala que se publica como **"lista no exhaustiva"**):

1. Tratamientos que impliquen **perfilado o valoración de sujetos**, incluida la recogida de datos del sujeto en múltiples ámbitos de su vida (desempeño en el trabajo, personalidad y comportamiento), que cubran varios aspectos de su personalidad o sobre sobre sus hábitos.
2. Tratamientos que **impliquen la toma de decisiones automatizadas** o que contribuyan en gran medida a la **toma de tales decisiones**, incluyendo decisión que impida el ejercicio de un derecho o el acceso a formar parte de un contrato.
3. Tratamientos que impliquen la **observación, monitorización, supervisión, geolocalización o control del interesado de forma sistemática y exhaustiva**, incluida la recogida de datos y metadatos a través de redes, aplicaciones o en zonas de acceso público, así como el **procesamiento de identificadores únicos** que permitan la **identificación de usuarios de servicios de la sociedad de la información** como pueden ser los servicios web, TV interactiva, aplicaciones móviles, etc.
4. Tratamientos que impliquen **el uso de categorías especiales de datos** a las que se refiere el artículo 9.1 del RGPD, datos relativos a **condenas o infracciones penales** a los que se refiere el artículo 10 del RGPD o datos que **permitan determinar la situación financiera o de solvencia** o **deducir información sobre personas con categorías especiales de datos**.
5. Tratamientos que impliquen **el uso de datos biométricos** para identificar de manera única a una persona física.
6. Tratamientos que impliquen **el uso de datos genéticos** para cualquier fin.
7. Tratamientos que impliquen **el uso de datos a gran escala**.
8. Tratamientos que impliquen la **asociación, combinación o enlace de registros de bases de datos de dos o más tratamientos con finalidades diferentes** o por responsables distintos.
9. Tratamientos de **datos de sujetos vulnerables** o en riesgo de exclusión social, datos de menores de 14 años, etc.
10. Tratamientos que **impliquen nuevas tecnologías o un uso innovador** de tecnologías consolidadas, incluyendo tecnologías a una nueva escala, que suponga nuevas formas de recogida y uso de datos con riesgo para los derechos y libertades.
11. Tratamientos de datos que **impidan a los interesados ejercer sus derechos**, utilizar un servicio o ejecutar un contrato, como por ej. tratamientos en los que los datos han sido recopilados por un responsable distinto al que los va a tratar y aplica alguna de las excepciones de los datos que deben proporcionarse a los interesados (art. 14.5 (b,c,d) del RGPD).

Fuente: https://www.aepd.es/media/criterios/listas-dpia-es-35-4.pdf

KEEP CODING

Cómo impacta el RGPD en los sistemas de las Empresas



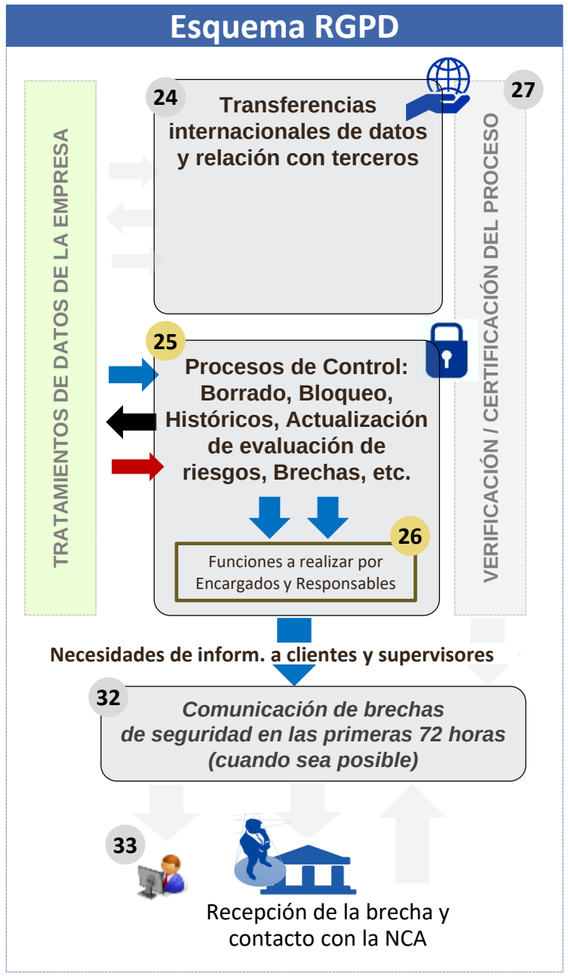
24 Las transferencias internacionales de datos a terceros ya estaban pautadas en la anterior ley de protección de datos, introduciéndose algunos cambios que no son los de mayor impacto del reglamento. En cualquier caso, es relevante conocer las obligaciones a este respecto:

- Los datos solo podrán ser comunicados fuera del Espacio Económico Europeo:
  - **A países, territorios o sectores específicos** (el RGPD incluye también organizaciones internacionales) sobre los que la **Comisión Europea** haya adoptado una decisión **reconociendo** que ofrecen un nivel de protección **adecuado**. (Criterios establecidos en el **artículo 45**). Estos países se revisarán con cierta periodicidad.

    Dicha transferencia no requerirá ninguna autorización específica
  - **Cuando se hayan ofrecido garantías adecuadas** sobre la protección que los datos recibirán en su destino (artículo 46). Esas garantías adecuadas podrán ser aportadas, sin que se requiera autorización expresa de una autoridad de control. Se amplían, además, la lista de "posibles instrumentos" para ofrecer garantías, incluyéndose expresamente, entre otras, las Normas Corporativas Vinculantes para responsables y encargados, los códigos de conducta y esquemas de certificación y las cláusulas contractuales modelo que puedan aprobar las autoridades de protección de datos.
  - **Cuando se aplique alguna de las excepciones** que permiten transferir los datos sin garantías de protección adecuada por razones de necesidad vinculadas al propio interés del titular de los datos o a intereses generales (artículo 49).
- En todo caso, las transferencias a terceros países y organizaciones internacionales **deben cumplir el Reglamento** y el responsable o encargado cumplirá las obligaciones de transferencia de datos personales a terceros países u organizaciones internacionales.

Se añade una excepción en la transferencia de datos a la LOPD previa: Se trata de la posibilidad de que el responsable pueda transferir datos a un país sin nivel adecuado de protección cuando esa transferencia sea **necesaria para satisfacer intereses legítimos** del responsable, y la transferencia no es repetitiva y **afecta sólo a un número limitado de interesados**. En todo caso, la transferencia solo será posible si no prevalecen los derechos, libertades e intereses de los afectados y **deberá comunicarse a la autoridad de protección de datos**.

Cómo impacta el RGPD en los sistemas de las Empresas



25 Aunque la responsabilidad última sobre el tratamiento de información sigue estando atribuida al responsable, que es quien determina la existencia del tratamiento y su finalidad, el RGPD introduce obligaciones dirigidas expresamente a los encargados y no únicamente a los responsables. Por ejemplo:

- Deben mantener un registro de actividades de tratamiento.
- Deben determinar las medidas de seguridad aplicables a los tratamientos que realizan.
- Deben designar a un Delegado de Protección de Datos en los casos previstos por el RGPD.

Los encargados pueden adherirse a códigos de conducta o certificarse en el marco de los esquemas de certificación previstos por el RGPD.

26 Los responsables habrán de elegir únicamente encargados que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del Reglamento.

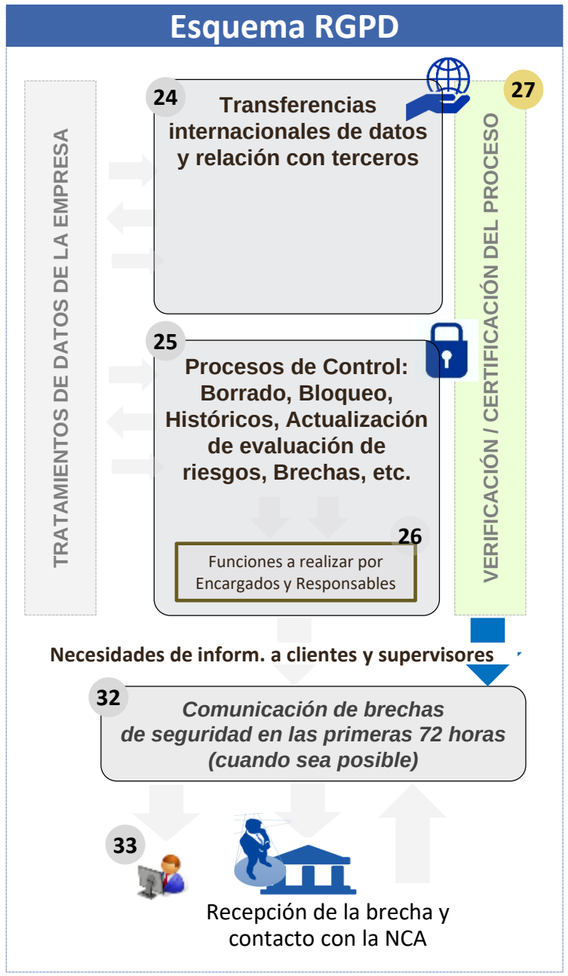
Las relaciones entre el responsable y el encargado deben formalizarse en un “contrato” / acto jurídico que vincule al encargado respecto al responsable.

Se regula de forma minuciosa el contenido mínimo de los contratos de encargo, que debe contener entre otros aspectos:

- Objeto, duración, naturaleza y la finalidad del tratamientos.
- Tipo de datos personales y categorías de interesados
- Obligación del encargado de tratar los datos personales únicamente siguiendo instrucciones documentadas del responsable
- Condiciones para que el responsable pueda dar su autorización previa, específica o general, a las subcontrataciones
- Asistencia al responsable, siempre que sea posible, en la atención al ejercicio de derechos de los interesados.

Los encargados del tratamiento, en resumen, serán responsables de poder aplicar el resto de obligaciones del reglamento que se han cubierto de forma aislada en otras capas, y que pueden derivar en acciones de bloqueo, borrado, aplicación de parches de seguridad, adaptaciones a modificaciones en los tratamientos, etc. Esto se traduce adicionalmente en responder ante el **“derecho al olvido”** que introduce el RGPD, que no está considerado un derecho autónomo o diferenciado de los clásicos derechos ARCO, sino la **consecuencia de la aplicación del derecho al borrado de los datos personales en un entorno online**.

Cómo impacta el RGPD en los sistemas de las Empresas



27 Debido a la complejidad y extensión de la normativa a prácticamente cualquier empresa, las autoridades nacionales están haciendo esfuerzos por facilitar **cuestionarios / herramientas de verificación del cumplimiento de la normativa**, con preguntas más o menos sencillos que pueden ser aplicables (y adaptarse más o menos) en función del tipo de organización.

A este respecto, la AEPD ha sacado un Listado de cumplimiento normativo en Abril de 2018 con **29 bloques** entre los que se encuentran los relacionados con la **transparencia** en la información a facilitar a los ciudadanos, el **ejercicio de derechos** por parte de estos, el registro de actividades, las **medidas de seguridad** o las **transferencias internacionales**. Unido a esto, cuenta con **dos tipos de Listados de Verificación**, uno estándar y otra versión simplificada, dentro de la Guía del RGPD para responsables de tratamiento.

Legitimación

- ¿Tiene establecida claramente cuál es la base legal de los tratamientos que realiza y ha documentado de alguna forma el modo en que la ha establecido?
- Si alguno de los tratamientos que realiza está basado en el consentimiento de los interesados, ¿ha verificado que ese consentimiento reúne los requisitos que exige el RGDP? En caso contrario, ¿ha previsto cómo recabar el consentimiento de forma adaptada al RGPD o ha encontrado otra base legal adecuada para esos tratamientos?

Información y derechos

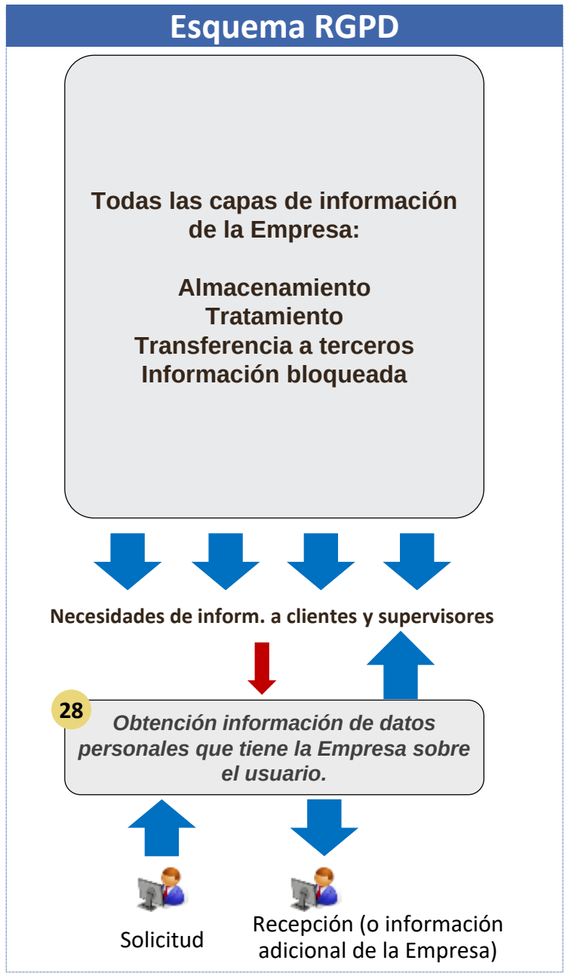
- La información que se proporciona a los interesados, ¿está presentada de forma clara, concisa, transparente y de fácil acceso?
- ¿Contiene esa información todos los elementos que prevé el RGPD?
- ¿Dispone de mecanismos para el ejercicio de derechos visibles, accesibles y sencillos? ¿Pueden ejercerse los derechos por vía electrónica?

…

Esto incluye las propias necesidades de certificación de las Empresas, en general respecto a su Delegado de Protección de Datos, pero también respecto a otras obligaciones del reglamento, estipuladas en el artículo 42:

- *Los Estados miembros, las autoridades, el Comité y la Comisión promoverán (…) la creación de mecanismos de certificación en materia de protección de datos y de **sellos y marcas de protección de datos** a fin de demostrar el cumplimiento de lo dispuesto en el presente Reglamento en las operaciones de tratamiento de los responsables y los encargados.*

Cómo impacta el RGPD en los sistemas de las Empresas



28 El derecho a la portabilidad de los datos es una **forma más avanzada del "derecho de acceso"** existente en la LOPD previa, por el cual la Empresa está obligada a **proporcionar una copia al interesado** en un **formato estructurado**, de uso común y que permita la lectura por ordenador. **Plazo de 1 mes** para responder (2 meses si es compleja), y entrega gratuitamente (salvo que sea reiterado)

Este requerimientos está **suponiendo un reto para las empresas** que tienen múltiples formatos de información del cliente, y sobre el que deben dar una respuesta que se adapte a cualquier petición de información. Incluso, la forma de dar acceso a estos datos, que pueden ser especialmente voluminosos, plantea dudas en la industria (desde proporcionar los datos en un espacio a través de internet, hasta proporcionarlo al cliente a través de un dispositivo externo (por ejemplo USB) a tal efecto).

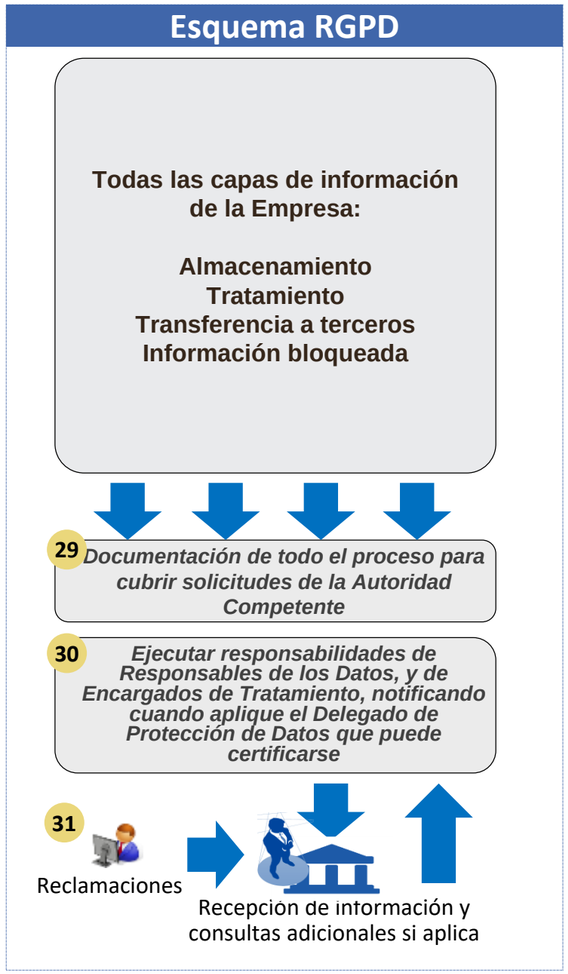
Este derecho **sólo deberá proporcionarse cuando**:	**No es aplicable cuando**:
- El tratamiento se efectúe **por medios automatizados**. - El tratamiento se base en el **consentimiento o en un contrato**. - El interesado lo solicita respecto a los datos **que haya facilitado *** al responsable y que le incumban, incluidos los datos derivados de la propia actividad del interesado.	- Se realice **debido a los datos de terceras personas** que un interesado haya facilitado a un responsable. - El interesado haya solicitado la portabilidad de datos que le incumban pero que **hayan sido proporcionados al responsable por terceros**.

* Los datos "facilitados" por el interesado **proceden también de la observación de sus actividades**, lo cual significa que debe incluir datos personales que se observan a partir de las actividades de los usuarios, tales como registros de actividad, historial de uso de sitios web o actividades de búsqueda, etc. según establece en un dictamen propio el Grupo de Trabajo del Artículo 29. Se trata de datos observados facilitados por el interesado en virtud del uso del servicio o dispositivo.

En cambio, **los datos inferidos y creados por el responsable del tratamiento** sobre la base de los datos facilitados por el usuario, en la medida en que son "originales", **no se considerarán facilitados por el usuario, y por tanto quedan fuera de esta obligación**.

Adicionalmente, el mismo Grupo de Trabajo aclara que, **cuando no existan formatos de uso común en un sector o contexto determinados, los responsables del tratamiento deben proporcionar los datos personales utilizando "formatos abiertos de uso común** (p. ej. XML, JSON, CSV,...) **junto con metadatos útiles** con el mejor nivel posible de granularidad, al tiempo que mantienen un alto grado de abstracción". Un PDF con correos electrónicos, por ejemplo, no conservaría los metadatos del correo.

Cómo impacta el RGPD en los sistemas de las Empresas



29 Si bien el RGPD va **más allá de rellenar documentación**, no puede obviarse que a partir del 25 de Mayo de 2018 la Empresa tiene la **obligación de demostrar que está cumpliendo el RGPD**, y eso va a suponer la actualización de políticas y procedimientos, así como un exhaustivo proceso de documentación de sus actividades de tratamiento, medidas de control, forma de obtener los consentimientos y tratarlos en los procesos de tratamiento de información, y resto de aspectos relevantes a cumplir.

30 Se crea una **nueva figura, el Delegado de Protección de Datos**, que ha de ser nombrado en algunas empresas atendiendo a sus cualificaciones profesionales y a su conocimiento de la legislación y la práctica de la protección de datos. Aunque no debe tener una titulación específica, se ele exigen tanto conocimientos jurídicos en la materia como en materia de tecnología aplicada al tratamiento de datos o en relación con el ámbito de actividad de la organización en la que el DPD desempeña su tarea.

La **designación del DPD y sus datos de contacto deben hacerse públicos** por los responsables y encargados, y deberán ser **comunicados a las autoridades de supervisión** competentes.

La designación del DPD en las organizaciones tiene que cumplir al menos los siguientes requisitos:

- Total autonomía en el ejercicio de sus funciones.
- Necesidad de que se relacione con el nivel superior de la dirección.
- Obligación de que el responsable o el encargado faciliten al DPD todos los recursos necesarios para desarrollar su actividad.

La AEPD ha optado por promover un sistema de certificación de profesionales de protección de datos, si bien no es obligatorio.

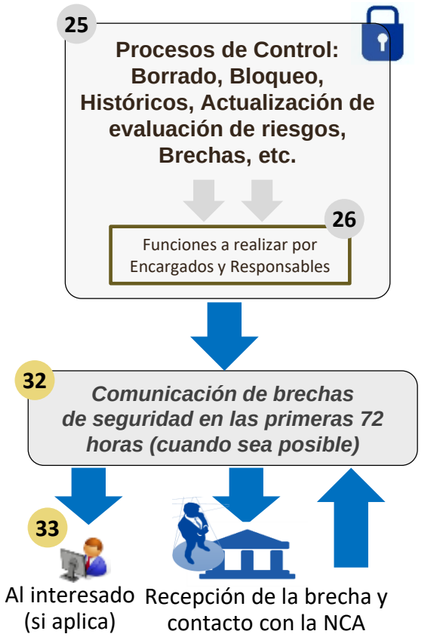
31 Una de las obligaciones que **no afecta de forma directa a las Empresas**, pues la reclamación no le llega propiamente a la Empresa, **pero sí de forma indirecta** (puede suponer un aumento del número de reclamaciones) es el **nuevo sistema de "ventanilla única"** que instaura el Reglamento General de Protección de Datos que permite a cualquier usuario **poner una reclamación relativa a la protección de datos en cualquier autoridad nacional competente, siendo esta autoridad la que se pondrá en contacto internamente con las otras autoridades que puedan estar afectadas** por la reclamación.

Anteriormente, no existía esta posibilidad, y era mucho más complejo para usuarios (por ejemplo, españoles) poder denunciar un problema de protección de datos que suponía una notificación a una autoridad extranjera,

Mayores obligaciones organizativas y de gobierno

Cómo impacta el RGPD en los sistemas de las Empresas

Esquema RGPD



32 Se conocen como "quiebras de seguridad" en el reglamento toda "*violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos*". (Artículo 4). Esto incluye sucesos como la pérdida de un ordenador portátil, el acceso no autorizado a las bases de datos de una organización (incluso por su propio personal) o el borrado accidental de registros que deben ser tratadas como el Reglamento establece.

El RGPD indica que "Si no se toman a tiempo medidas adecuadas, las violaciones de la seguridad de los datos personales pueden entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas" (considerando 85). Por ello, introduce una **nueva obligación de notificación a la Autoridad Nacional Competente**:

- *"tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales, el responsable debe, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales a la autoridad de control competente, a menos que el responsable pueda demostrar (…) la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas. Si dicha notificación no es posible en 72 horas, debe acompañarse de una indicación de los motivos de la dilación, pudiendo facilitarse información por fases". (Considerando 85).*

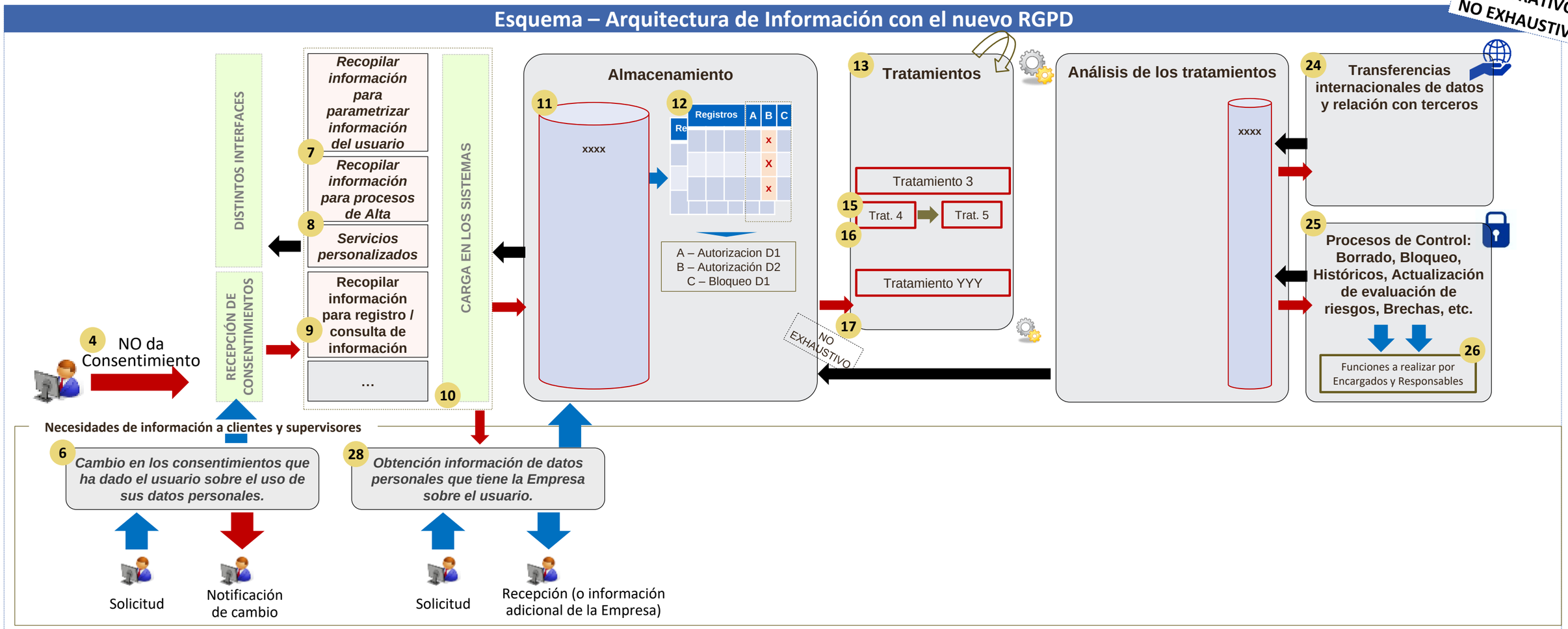
33 En el caso de que **pueda entrañar un alto riesgo** para los derechos y libertades del interesado, el responsable del tratamiento debe **comunicar al interesado** sin dilación indebida la violación de la seguridad de sus datos personales y así permitirle tomar las precauciones necesarias.

- *"La comunicación debe describir la naturaleza de la violación de la seguridad de los datos personales y las recomendaciones para que la persona física afectada mitigue los potenciales efectos adversos resultantes de la violación. Estas comunicaciones a los interesados deben realizarse tan pronto como sea razonablemente posible y en estrecha cooperación con la autoridad de control" (Considerando 86).*

Las Autoridades Competentes y los interesados recibirán más notificaciones ante brechas de seguridad

Dónde se complica todo – Los consentimientos deben propagarse a todo el flujo de información de la Empresa, y no se gestionan en un único momento

EJEMPLO ILUSTRATIVO NO EXHAUSTIVO



Guía - Código de Buenas Prácticas - Protección de Datos - Big Data

La AEPD, consciente de la relevancia de establecer pautas en los nuevos modelos de explotación de datos, ha publicado un código de buenas prácticas en protección de datos para proyectos big data realizado con la colaboración de diferentes empresas:

FASE BIG DATA	ESTRATEGIA	IMPLEMENTACIÓN
Adquisición y recolección	Minimizar	• Seleccionar antes de adquirir • EIPD
	Agregar	• Anonimización en la fuente origen
	Ocultar	• Herramientas de cifrado • Herramientas de enmascaramiento de datos
	Informar	• Transparencia - Comunicación al interesado
	Controlar	• Mecanismos para recabar consentimiento
Análisis y validación	Agregar	• Técnicas de anonimización
	Ocultar	• Herramientas de cifrado
Almacenamiento	Ocultar	• Herramientas de cifrado • Mecanismos de autenticación y control de acceso
	Separar	• Almacenamiento distribuido / descentralizado
Explotación	Agregar	• Técnicas de anonimización
Todas las fases	Cumplir / Demostrar	• Definición de políticas • Trazabilidad de las acciones • Herramientas de cumplimiento

- Probablemente el aspecto más relevante de la guía y de mayor aplicación práctica son las **estrategias de privacidad más adecuadas** que se recomiendan para **cada fase** de uso de los datos, teniendo en cuenta las fases que suele tener un proyecto de Big Data, y las **medidas que pueden implementarse** para cumplir esas estrategias.

- Al margen de todas las técnicas de anonimización y seguridad que pueden incorporarse por fase, el Código de buenas prácticas recomienda la **adopción de medidas de responsabilidad proactiva** que vayan más allá de un enfoque de cumplir requerimientos “tasados” en una normativa.

- Se recomienda el **uso de diversas certificaciones de privacidad**, existentes tanto a nivel nacional como internacional. Aunque muchas no están acreditadas oficialmente. Una de las citadas en el informe como la **certificación de privacidad más conocida en Europa, es EuroPriSe**, que ofrece certificaciones para productos y servicios IT que cumplen con la legislación europea de protección de datos.

Fuente: https://www.aepd.es/media/guias/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf

Adaptación al RGPD

- Cumplir el Reglamento General de Protección de Datos puede ser más o menos complejo en función de los datos tratados y tipo de organización:

RGPD FACILITA — HERRAMIENTA PARA TRATAMIENTOS DE ESCASO RIESGO

Si su organización realiza alguno de los siguientes tratamientos, márquelo:

- ☐ Hacer o analizar perfiles
- ☐ Hacer publicidad y prospección comercial masiva a potenciales clientes
- ☐ Prestación de servicios de explotación de redes públicas o servicios de comunicación electrónica (proveedor de servicios de internet (LGT))
- ☐ Gestionar los asociados o miembros de partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical
- ☐ Gestión, control sanitario o venta de medicamentos
- ☐ Historial clínico o sanitario
- ◉ Ninguna de las anteriores

Ha respondido de forma negativa a todas las cuestiones anteriores, por tanto, se podría entender que los tratamientos realizados por su entidad entrañan, a priori, un escaso nivel de riesgo para los derechos y libertades de los interesados y por tanto se encontraría en disposición de utilizar el siguiente programa.

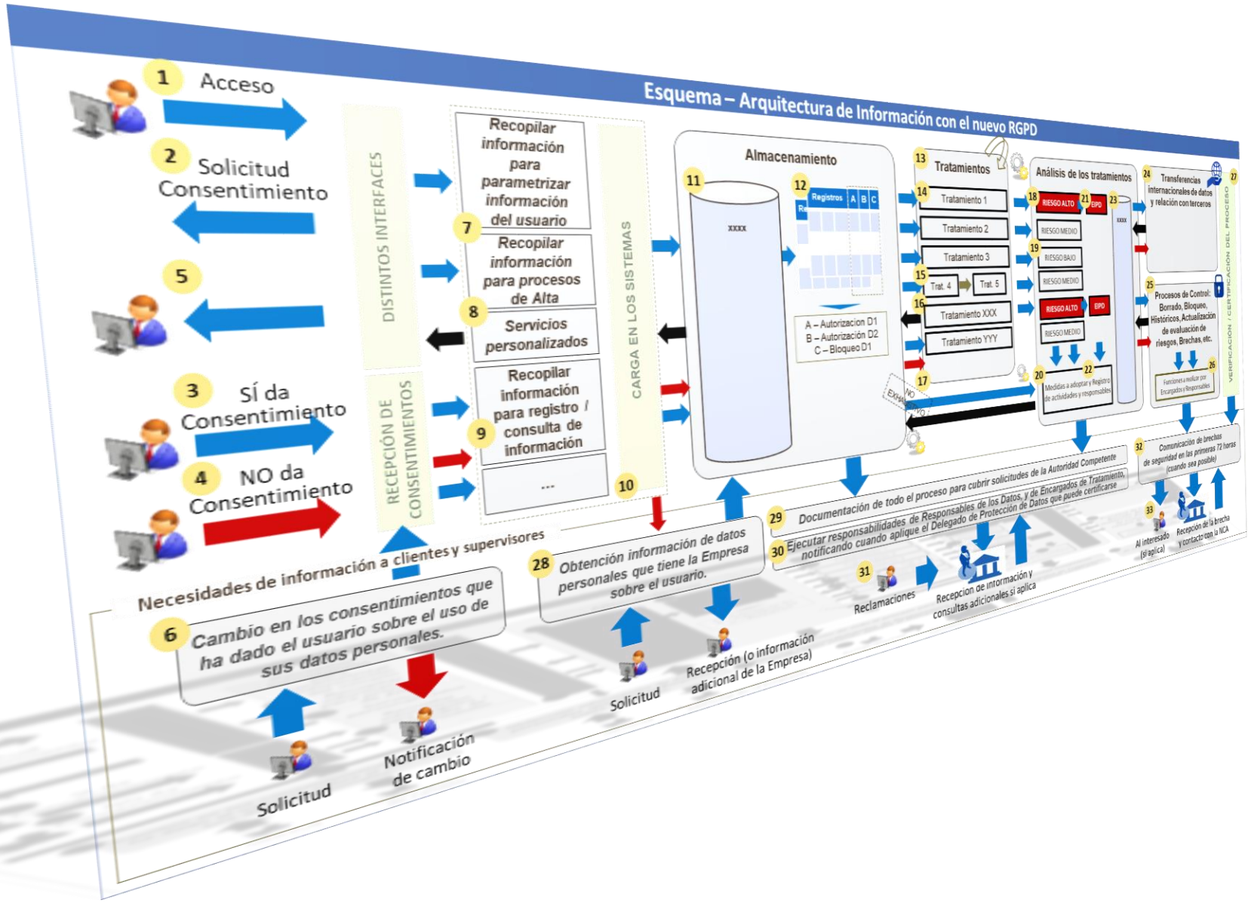
ADAPTACIÓN AL RGPD – Sector Privado

1. ***Designar DPD (si aplica) o sino identificar responsable de coordinar la adaptación al RGPD***
2. ***Elaborar el REGISTRO ACTIVIDADES DE TRATAMIENTO (servicio de solicitud de copia de la inscripción), teniendo en cuenta su finalidad y la base jurídica***
3. ***Realizar un ANÁLISIS DE RIESGOS***
4. ***Revisar MEDIDAS DE SEGURIDAD a la luz de los resultados del análisis de riesgos***
5. ***Establecer mecanismos y procedimiento de NOTIFICACIÓN DE QUIEBRAS DE SEGURIDAD***
6. ***A partir de los resultados del análisis de riesgos, realizar, en su caso, una EVALUACIÓN DE IMPACTO EN LA PROTECCIÓN DE DATOS***

Otras — ***Adecuar los formularios (derecho de información), Adaptar los MECANISMOS Y PROCEDIMIENTOS para el ejercicio de derechos, Valorar si los ENCARGADOS ofrecen garantías y adaptación de contratos y Elaborar / Adaptar POLÍTICA DE PRIVACIDAD***

KEEP CODING

Conclusiones



- Cumplir el Reglamento General de Protección de Datos **no puede suponer rellenar un "Check-box"** indicando que no existen riesgos.
- El **enfoque proactivo**, y no únicamente reactivo, introduce un **mayor nivel de exigencia** transversal a los requerimientos de protección de datos que ya existían por la LOPD previa, siendo un sistema vivo en el que los usuarios pueden dar y quitar su consentimiento.
- Es necesario tener en cuenta que existen responsables y encargados de tratamiento con responsabilidades específicas, con **transcendencia suficiente** para poder adoptar decisiones de protección de datos en función del riesgo de los tratamientos.
- No tener fugas de datos / brechas de seguridad **no justifica un uso indiscriminado** de datos personales: El consentimiento del cliente a un servicio **no supone un consentimiento a cualquier uso** que quiera realizar el tercero de sus datos.
- Los **problemas de seguridad que ocurran deberán ser notificados** a las Autoridades Competentes (y, en ocasiones, a los propios interesados) en un plazo breve (<72 horas), por lo que no podrán mantenerse en privado.

Autoevaluación

1. *Consentimiento – ¿En qué casos / Cuándo / Cómo?*
2. *¿Cuáles son los datos protegidos? ¿Qué significa que identifiquen?*
3. *¿Derechos del cliente?*
4. *¿Cuándo notifico las brechas de seguridad, cuáles, y a quién?*
5. *¿Cuándo mis actividades son de riesgo alto y cómo mitigar los riesgos?*
6. *¿Cuándo realizar evaluación de impacto de riesgo (EIPD / PIA)?*
7. *Responsable – DPO, Supervisores y posibles sanciones*
8. *¿Cuáles son las estrategias de diseño de la privacidad más comunes?*
9. *¿Me puedo llevar todos mis datos a otro sitio? ¿Portabilidad? ¿Responsabilidad en el Diseño y por defecto?*
10. *¿Cuándo aplica RGPD? ¿Falta algo?*

¡Gracias!