Protección de Datos Personales y GDPR

BE SAFE ON THE INTERNET

Co-funded by the Erasmus+ Programme of the European Union

Index

1. Introducción 6

2. GDPR 7

2.1. Principios del GDPR 8

2.2. Usar, procesar, almacenar y transferir datos en UE 9

2.3. Consentimiento respecto al procesamiento de datos 11

2.4. Derecho al acceso y a la portabilidad de datos 14

2.5. Violaciones de datos 15

2.6. Multas 15

2.7. Preparaciones para el cumplimiento del GDPR 16

3. ePrivacidad 20

3.1. Puntos clave de la propuesta de la Comisión Europea 21

3.2. Reglas de privacidad más estrictas para las comunicaciones electrónicas. 22

3.3. Ley aplicable y situaciones transfronterizas 24

3.4. Relación entre el GDPR y ePR 24

3.5. Beneficios para ciudadanos y empresas 24

4. Protección de datos personales 25

4.1. ¿Qué regulaciones complementan las regulaciones europeas? 26

4.1.1. Austria 26

4.1.2. República Checa 27

4.1.3. Portugal 28

4.1.4. España 30

5. Datos no personales 35

5.1. Libre circulación de datos dentro de la UE 36

5.2. Porting of data 37

5.3. Procedure for cooperation between authorities 38

5.4. Disponibilidad de datos para autoridades competentes 38

5.5. Sanciones por infracciones 38
6. Catálogo de contenido sistematizado 39
7. Conclusiones 40
8. Referencias **41**

Lista de abreviaciones

DPA: Data Protection Authority (Autoridad de Protección de Datos)

DPO: Data Protection Officer (Delegado de Protección de Datos)

DSG: Ley de protección de datos austriaca Datenschutzgesetz

DSVGO: Datenschutz-Grundverordung alemana

EEA: European Economic Area (Área Económica Europea)

ePR: Regulación de ePrivacidad

EU/UE: European Union/Unión Europea

GDPR: General Data Protection Regulation (Reglamento General de Protección de Datos)

Figures

Figura 1 - GDPR 7
Figura 2 - Principios of GDPR 8
Figura 3 - Procesar datos personales 9
Figura 4 - Controlador y procesador de datos 10
Figura 5 - Procesar datos personales 12
Figura 6 - Ejemplo de consentimiento 13
Figura 7 - Derechos bajo el GDPR 14
Figura 8 - Cumplimiento del GDPR 16
Figura 9 - reglas de ePrivacidad 22
Figura 10 - Protección de la privacidad online 23
Figura 11 - GDPR vs ePR 24
Figura 12 - Benecios para ciudadanos y empresas 25
Figura 13 - Datos no personales 35

Tables

Table 1 – Legislación de protección de datos personales 32

1. Introducción

Hoy en día, el mundo depende cada vez más de los datos porque los datos pueden agregar un valor significativo a numerosos agentes económicos. En la Unión Europea (UE), existen regulaciones con respecto a los datos personales: el Reglamento (UE) 2016/679 (Reglamento general de protección de datos) y el Reglamento de privacidad electrónica (ePR) que es una propuesta para la Directiva de privacidad y comunicaciones electrónicas 2002 (ePrivacy Directiva 2002/58 / CE).

El Reglamento (UE) 2018/1807 tiene como objetivo eliminar los obstáculos relacionados con la libre circulación de datos no personales entre los estados miembros de la UE y la Tecnología de la Información en Europa. Junto con el Reglamento General de Protección de Datos (GDPR), este reglamento garantiza un enfoque integral y coherente para la libre circulación de todos los datos en Europa. El alcance que pretende lograr el ePR es reforzar la confianza y la seguridad en el mercado único digital mediante la actualización del marco legal sobre ePrivacidad (ePR).

Estas tres regulaciones se aplican a cada país europeo a pesar de que hay algunas cláusulas de apertura que dejan un margen de maniobra a los legisladores nacionales.

En este informe puede encontrar la información más importante relacionada con esta legislación. Además, en este documento discutiremos cómo se ha adaptado la legislación europea sobre protección de datos personales en Austria, España, Portugal y la República Checa.

2. GDPR

El GDPR (Reglamento (UE) 2016/679) es una ley de la UE sobre protección de datos y privacidad para todos los ciudadanos individuales de la UE y el Espacio Económico Europeo (EEE). También aborda la exportación de datos personales fuera de las áreas geográficas mencionadas anteriormente. El GDPR está en vigor desde mayo de 2018 y tiene tres objetivos principales:

a) **Armonizar las leyes de privacidad de datos** en toda Europa;
b) Proteger y potenciar la privacidad de los datos de todos los ciudadanos de la UE;
c) Cambiar la forma en que las organizaciones de la región abordan la privacidad de los datos.

Figura 1 - GDPR

Fuente: Business2Community (2019)

Con el GDPR, Europa está señalando su postura firme sobre la privacidad y la seguridad de los datos y el GDPR reestructura la forma en que las empresas/organizaciones gestionan los datos. El GDPR se aplica a:

a) Una **empresa o entidad que procesa datos personales como parte de las actividades de una de sus sucursales establecidas en la UE,** independientemente de dónde se procesen los datos; o,

b) Una **empresa o entidad establecida fuera de la UE que ofrece bienes/servicios** (de pago o gratuitos) o que supervisan el comportamiento de las personas en la UE.

2.1. Principios del GDPR

El GDPR tiene algunos principios generales con respecto al proceso de datos personales. Uno de estos principios requiere que los datos se procesen de manera transparente, lo que significa que este proceso debe ser claro y legítimo. Además, la cantidad de datos procesados debe mantenerse al mínimo, y dependiendo del propósito, los datos deben ser precisos y el tiempo de almacenamiento debe limitarse a un período que esté relacionado con el propósito. Además, se debe proteger la integridad y la confidencialidad de los datos. Los principales principios del GDPR están presentes en la siguiente figura.

Figura 2 - Principios of GDPR

Fuente: I-scoop (2019)

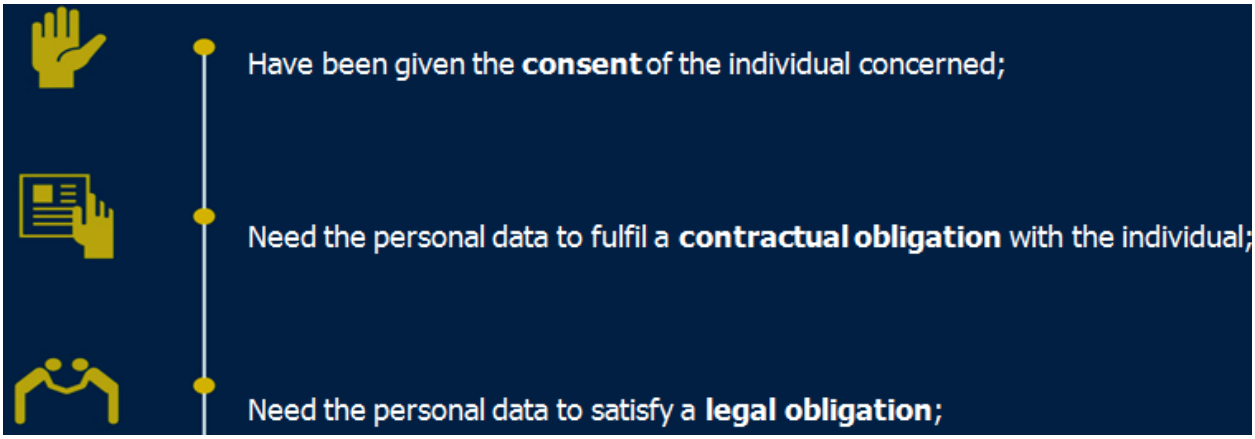
En general, el principal punto de contacto para preguntas sobre protección de datos es la Ley de Protección de Datos (DPA) en cada estado miembro de la UE donde se encuentra su empresa/organización. Sin embargo, si su empresa/organización procesa datos en diferentes estados miembros de la UE o es parte de un grupo de empresas establecidas en diferentes estados miembros de la UE, el principal punto de contacto puede ser un DPA en otro estado miembro de la UE.

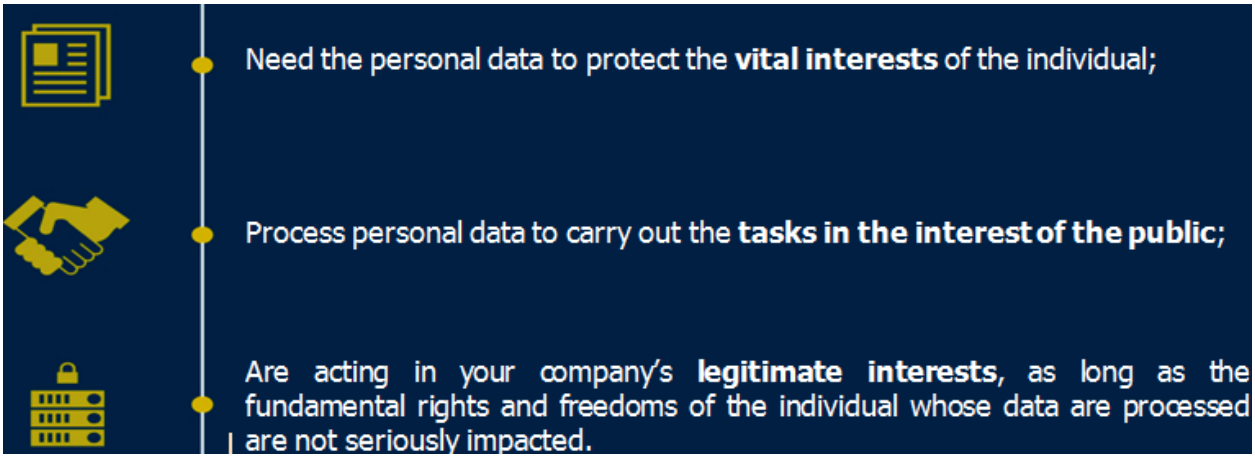
Encuentre su Autoridad Nacional de Protección de Datos en:
https://edpb.europa.eu/about-edpb/board/members_en

2.2. Usar, procesar, almacenar y transferir datos en UE

Como individuo, empresa u organización, tiene derecho a usar, recopilar, almacenar, transferir o administrar datos personales y a usar centros de datos o servicios en la nube en cualquier lugar de la UE. Las reglas para tratar datos personales difieren de las reglas para los datos no personales. Sin embargo, los datos personales y no personales a menudo se recopilan y almacenan juntos y esto se conoce como datos mixtos. Hay algunos puntos que las empresas/organizaciones deben cumplir al procesar los datos personales que están presentes en la siguiente figura.

Figura 3 - Procesar datos personales





Fuente: European Commission (2019)

Durante el procesamiento, los datos personales pueden pasar a través de diferentes compañías u organizaciones y dentro de este ciclo hay dos perfiles principales que se ocupan del procesamiento de datos personales: el controlador de datos y el procesador de datos.

Figura 4 - Controlador y procesador de datos

Controlador de datos: decide el propósito y la forma en que se procesan los datos personales

Procesador de datos: retiene y procesa datos en nombre de un controlador de datos

Fuente: Own elaboration

Las empresas/organizaciones que procesan datos están obligadas a mantener registros de las actividades de procesamiento, a menos que tengan menos de 250 empleados. Además, las empresas/organizaciones tienen que designar un Oficial de Protección de Datos (DPO) cuando se aplica uno de los siguientes aspectos:

- Cuando el procesamiento lo realiza un organismo público (excepto los tribunales);
- Cuando las actividades centrales del procesador "consisten en operaciones de procesamiento que, en virtud de su naturaleza, su alcance y/o sus propósitos, requieren un monitoreo regular y sistemático de los interesados a gran escala";
- Cuando se procesan categorías especiales de datos o "datos relacionados con condenas y delitos penales".

El DPO es alguien que puede haber sido designado por la compañía y es responsable de monitorear cómo se procesan los datos personales y de informar y asesorar a los empleados que procesan datos personales sobre sus obligaciones. El DPO puede ser un miembro del personal de su organización o puede ser contratado externamente sobre la base de un contacto de servicio. El DPO también coopera con la Autoridad de Protección de Datos (DPA) que sirve como punto de contacto con la DPA y los ciudadanos.

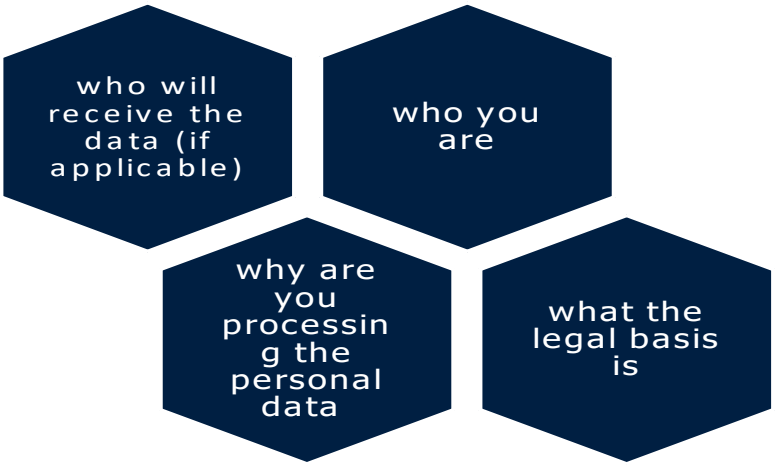
2.3. Consentimiento respecto al procesamiento de datos

La responsabilidad de cumplir con el GDPR depende de las empresas/organizaciones que procesan datos personales. Teniendo en cuenta la naturaleza, el alcance, el contexto y los propósitos del procesamiento, así como la severidad de los derechos y libertades de los ciudadanos, el controlador implementará medidas técnicas y organizativas apropiadas para garantizar y poder demostrar que el procesamiento se realiza de acuerdo con esta regulación. Esas medidas serán revisadas y actualizadas si es necesario. Ejemplos de estas medidas son seudonimización o encriptación.

El GDPR aplica reglas estrictas para procesar datos basados en el consentimiento. El propósito de estas reglas es asegurar que el individuo entienda lo que está

consintiendo. Esto significa que el consentimiento debe ser otorgado libremente por un acto afirmativo, como marcar una casilla en línea o firmar un formulario. Cuando alguien consiente el procesamiento de sus datos personales, solo puede procesar los datos para los fines para los que se dio el consentimiento. También es importante decir que debe proporcionar claramente a las personas información sobre quién procesa los datos personales sobre ellos y los motivos. Por ejemplo, la siguiente figura debe incluirse como mínimo:

Figura 5 - Procesar datos personales



Fuente: European Commission (2019)

En algunas situaciones, la información que proporcione también debe indicar:

- La información de contacto del DPO (si corresponde);
- Cuál es el interés legítimo que persigue la empresa cuando confía en este fundamento legal para el procesamiento;
- Las medidas aplicadas para transferir los datos a un país fuera de la UE;
- Durante cuánto tiempo se almacenarán los datos;
- Los derechos de protección de datos del individuo;
- Cómo se puede retirar el consentimiento (cuando el consentimiento es el fundamento legal para el procesamiento);
- Si existe una obligación legal o contractual de proporcionar los datos;

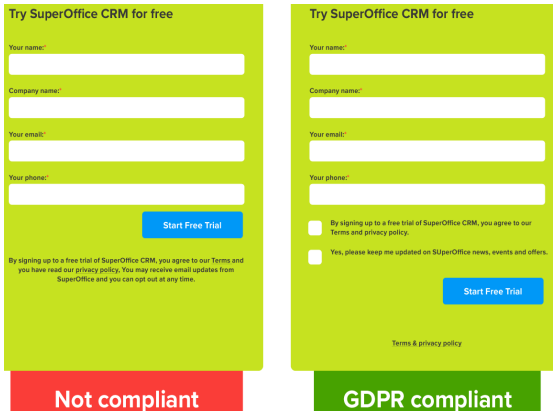
- En el caso de la toma de decisiones automatizada, información sobre la lógica, el significado y las consecuencias de la decisión.

Es importante tener en cuenta que esta información debe ser clara y debe usar un lenguaje simple/claro.

Las condiciones para el consentimiento se han fortalecido y las compañías/organizaciones ya no pueden usar términos largos e ilegibles y condiciones llenas de términos y conceptos legales. La solicitud de consentimiento debe presentarse de forma inteligible y de fácil acceso, con el propósito de procesar los datos adjuntos a dicho consentimiento. El consentimiento debe ser claro y distinguible de otros asuntos y debe proporcionarse en una forma e idioma inteligible y fácilmente accesible.

La siguiente figura muestra un ejemplo de lo que debe hacerse. En la siguiente figura, puede ver que el GDPR ha cambiado muchas cosas para las empresas/organizaciones. Por lo tanto, las empresas deben revisar sus procesos comerciales, aplicaciones y formularios para cumplir con el marketing por correo electrónico, por ejemplo. Para suscribirse a la comunicación, los prospectos deberán completar un formulario o marcar una casilla y luego confirmar que fueron sus acciones en otro correo electrónico.

Figura 6 - Ejemplo de consentimiento



Fuente: SuperOffice (2019)

2.4. Derecho al acceso y a la portabilidad de datos

Las empresas y organizaciones deben garantizar que las personas tengan derecho a acceder a sus datos personales de forma gratuita. Si recibe dicha solicitud, debe:

- Informarles si está procesando sus datos personales;
- Informarles sobre el procesamiento (el propósito del procesamiento, las categorías de datos personales en cuestión, etc.);
- Darles una copia de los datos personales que se procesan (en un formato accesible).

Con el nuevo GDPR, se vuelve más importante informar al cliente o la persona cuyos datos procesa sobre lo que sucede con los mismos. Los derechos que debe tener en cuenta se resumen en la siguiente figura.

Figura 7 - Derechos bajo el GDPR

Fuente: Serveit (2019)

Estos derechos se otorgan a las personas para proteger sus vidas privadas y controlar las huellas digitales que dejan al usar aplicaciones y servicios basados en Internet. Estos derechos están destinados a crear apertura, control y confianza entre todas las partes.

2.5. Violaciones de datos

Una violación de datos es cuando los datos personales se revelan, ya sea accidental o ilegalmente, a destinatarios no autorizados que no están disponibles temporalmente o se modifican.

Si ocurre una violación de datos y la violación representa un riesgo para los derechos y libertades individuales, debe notificar a su DPA dentro de las 72 horas después de darse cuenta de la violación.

2.6. Multas

Las multas se hacen más grandes y las líneas de tiempo se hacen más cortas. Según el RGPD, las notificaciones de incumplimiento ahora son obligatorias en todos los miembros donde es probable que una violación de datos "genere un riesgo para los derechos y libertades de las personas". Esto debe hacerse dentro de las 72 horas posteriores a la primera toma de conciencia de la infracción. Los procesadores de datos también deben notificar a sus clientes, los controladores sin demora indebida, después de darse cuenta por primera vez de una violación de datos.

Por lo tanto, el GDPR introduce un régimen de aplicación más estricto y expone a las entidades a una mayor responsabilidad financiera. Varios casos de alto nivel están en curso y podrían causar multas de hasta el 4% del anual de un negocio si hay una infracción grave. La multa máxima es de 20 millones de euros o el 4% de los ingresos mundiales, lo que sea mayor. Las autoridades de protección de datos también pueden emitir sanciones como prohibiciones en el procesamiento de datos o reprimendas públicas.

Bajo GDPR, las multas son administradas por el regulador de protección de datos en cada país de la UE. Se evaluará el total final de las multas y en qué cantidad:

gravedad y naturaleza; intención; mitigación; medidas de precaución; historia; cooperación; categoría de datos; notificación; Certificación; factores agravantes/atenuantes. Si los reguladores determinan que una organización tiene múltiples violaciones de GDPR, solo será penalizada por la más grave, siempre que todas las infracciones sean parte de la misma operación de procesamiento.

2.7. Preparaciones para el cumplimiento del GDPR

La aplicación de GDPR impone requisitos estrictos sobre la forma en que las empresas/organizaciones recopilan, almacenan y administran datos personales. Teniendo esto en cuenta, el GDPR proporciona a los ciudadanos de la UE un mayor control sobre sus datos personales y garantiza que su información esté protegida de forma segura en toda Europa, independientemente de si el procesamiento de datos se realiza en la UE o no.

El RGPD abarca tres áreas principales que toda empresa debe tener en cuenta (consulte la figura 5):

1. La propia regulación **GDPR**;
2. Los **sistemas** que utiliza para almacenar todos los datos de sus clientes;
3. Los **aspectos legales** de la regulación y cómo afectará la forma en que maneja los datos personales.

Figura 8 - Cumplimiento del GDPR

Fuente: Own elaboration

Además, un componente clave de la legislación GDPR es la privacidad por diseño. La privacidad por diseño requiere que todos los departamentos de una empresa/organización observen de cerca sus datos y cómo los manejan. Hay muchos temas que una empresa tiene que hacer para cumplir con GDPR. Encuentre algunos pasos que pueden ayudar a comenzar este proceso.

1. **Asigne los datos de su empresa:** Asigne de dónde provienen todos los datos personales de su empresa y documente lo que hace con los datos. Identifique dónde residen los datos, quién puede acceder a ellos y si existen riesgos asociados a los datos que posee.

2. **Determine qué datos necesita conservar:** GDPR fomenta un tratamiento más disciplinado de los datos personales. Por eso, es crucial mantener solo la información que sea necesaria y eliminar cualquier dato que no esté utilizando. Si su empresa/organización ha recopilado una gran cantidad de datos sin ningún beneficio/uso real, es el momento de considerar qué datos son importantes para su empresa/organización. En el proceso de limpieza puede seguir las preguntas siguientes:
   - ¿Por qué exactamente estamos archivando estos datos en lugar de simplemente borrarlos?
   - ¿Por qué estamos guardando todos estos datos?
   - ¿Qué estamos tratando de lograr al recopilar todas estas categorías de información personal?
   - ¿La ganancia financiera de eliminar esta información es mayor que encriptarla?

3. **Establezca medidas de seguridad:** desarrolle e implemente salvaguardas en toda su infraestructura para ayudar a contener cualquier violación de datos. Esto significa implementar medidas contra las violaciones de datos y tomar medidas

rápidas para notificar a las personas y las autoridades en caso de que ocurra una violación.

4. **Revise su documentación:** según el GDPR, las personas deben consentir explícitamente la adquisición y el procesamiento de sus datos. Las casillas marcadas previamente y el consentimiento implícito ya no serán aceptables.

2.8. Conocimiento del GDPR: un año después de la implementación

Después de un año de implementación del GDPR, el cambio más importante y significativo en el marco legal de protección de datos, los ciudadanos europeos son cada vez más conscientes de los derechos y deberes de la aplicación de la legislación de protección de datos personales.

Según los resultados publicados en junio de 2019 del informe "Reglamento general de protección de datos" realizado por la Comisión Europea, la mayoría (más de dos tercios) de los europeos han oído hablar del GDPR y también han oído hablar de los derechos garantizados por el GDPR, con la excepción del derecho a opinar cuando las decisiones están automatizadas (41%). Además, los países que conocen más el GDPR son: Suecia (90%), Países Bajos (87%) y Polonia (86%). Además, los encuestados de entre 25 y 54 años (75%) tienen más probabilidades de haber oído hablar del GDPR, los encuestados de entre 15 y 54 años tienen más probabilidades que los de 55 años o más de conocer sus derechos de datos personales y los hombres tienen más probabilidades de tener en cuenta cada uno de estos derechos en comparación con las mujeres. Cuanto más tiempo permanezca un encuestado en educación, más probabilidades tendrá de conocer esta legislación.

Además, Irlanda, Eslovaquia y Polonia tienen algunas de las proporciones más altas de encuestados que han oído hablar del GDPR y saben de qué se trata, y también las proporciones más altas de encuestados que han oído hablar de todos los derechos sobre los que se preguntó en la encuesta realizada.

En cuanto a la conciencia de las autoridades públicas nacionales a cargo de la protección de datos, la mayoría (6 de cada 10) dice haber escuchado sobre la

existencia de la autoridad pública en su país responsable de proteger sus derechos con respecto a sus datos personales.

Desde 2018, las autoridades nacionales de protección de datos están a cargo de hacer cumplir las nuevas normas y coordinan mejor sus acciones. Sin embargo, todavía queda trabajo por hacer en lo que respecta a los problemas de cumplimiento porque este es un proceso dinámico.

Según el informe legal de Deloitte "El GDPR: Seis meses después de la implementación: perspectivas del profesional", todavía hay trabajo por hacer con respecto a la implementación del GDPR. Las conclusiones más importantes de este informe sugieren que es importante:

- Lo primero que debe hacer cuando se trata de cumplir con el GDPR es conocer los detalles sobre el procesamiento de datos personales porque todavía hay una falta de conocimiento de las reglas básicas;
- Mejorar la transparencia sobre el procesamiento de datos personales con los interesados según lo requerido por el GDPR;
- Mejorar la orientación, las recomendaciones o los cargos oficiales del supervisor de protección de datos del país;
- Llevar a cabo capacitaciones de sensibilización del personal e involucrar a todas las personas con los requisitos GDPR más relevantes porque todos necesitan comprender cómo aplicarlo e implementarlo en su trabajo diario;
- La introducción de medidas de seguridad que van más allá de los estándares mínimos requeridos (por ejemplo, el cifrado de todos los documentos adjuntos al correo electrónico);
- Crear una plataforma no comercial para compartir conocimientos jurídicos especializados, buenas prácticas y soluciones prácticas y creativas entre especialistas en protección de datos personales;
- Directrices para pequeñas y medianas empresas con el fin de ayudarlas a aplicar en la práctica una nueva normativa legal sobre protección de datos personales;

- Creación de varias plantillas para tratar varios problemas relacionados con el GDPR (recopilar, implementar y transferir protección de datos personales y solicitar permiso para transferir datos personales;
- Desarrollo de algunas iniciativas dirigidas a escuelas y materiales de capacitación desde las primeras etapas.

3. ePrivacidad

La estrategia del mercado único digital tiene como objetivo aumentar la confianza y la seguridad de los servicios digitales. La reforma del marco de protección de datos, en particular la adopción del GDPR, fue una acción clave para esto. La Estrategia para el Mercado Único Digital también anunció la revisión de la Directiva 2002/58 / CE (Directiva sobre privacidad electrónica) para proporcionar un alto nivel de protección de la privacidad a los usuarios de servicios de comunicaciones electrónicas.

La Directiva sobre privacidad electrónica establece algunas normas que garantizan la protección de la privacidad en el sector de las comunicaciones electrónicas. Las comunicaciones electrónicas incluyen correo electrónico; aplicaciones; teléfono; Mensajería instantánea; correo no deseado; marketing directo; empresas de telecomunicaciones; desarrolladores de aplicaciones móviles; redes de publicidad en línea entre muchos otros. Esta directiva también proporciona protección para usuarios y suscriptores de servicios de comunicaciones electrónicas contra comunicaciones no solicitadas.

La directiva de privacidad electrónica exige que los proveedores de servicios de comunicaciones electrónicas, como el acceso a Internet y los teléfonos fijos y móviles:

a) Tomar las medidas apropiadas para salvaguardar la seguridad de los servicios de comunicaciones electrónicas;

b) Garantizar la confidencialidad de las comunicaciones y los datos de tráfico relacionados en las redes públicas.

Los **tres objetivos principales de la directiva de privacidad electrónica** son los siguientes:

- Garantizar un nivel equivalente de protección en toda la UE del derecho fundamental a la privacidad y la confidencialidad con respecto al procesamiento de datos personales en el sector de las comunicaciones electrónicas. Esta protección también se otorga a los suscriptores que son personas jurídicas;
- Garantizar un nivel equivalente de protección con respecto al procesamiento de datos personales en el sector de las comunicaciones electrónicas para proteger el derecho fundamental a la protección de datos;
- Garantizar la libre circulación de datos personales procesados en el sector de las comunicaciones electrónicas y la libre circulación de equipos y servicios terminales de comunicaciones electrónicas en la UE.

El ePR reemplazará la directiva de privacidad electrónica existente de la UE y la directiva de comunicaciones electrónicas 2002. Esta regulación es importante porque significa que será un acto legal y exigible en su totalidad en todos los estados miembros como GDPR. Además, esta propuesta debe garantizar la coherencia con el GDPR.

Si bien el GDPR garantiza la protección de los datos personales, el ePR tiene como objetivo garantizar la confidencialidad de las comunicaciones que también pueden contener datos no personales y datos relacionados con una persona jurídica.

El ePR debía entrar en vigor el 25 de mayo de 2018 junto con el GDPR, sin embargo, la continua deliberación y el cabildeo de algunos han retrasado la aplicación de este reglamento.

3.1. Puntos clave de la propuesta de la Comisión Europea

La propuesta de un reglamento sobre normas de alto nivel de privacidad para todas las comunicaciones electrónicas incluye:

Figura 9 - reglas de ePrivacidad

Fuente: European Commission (2019)

3.2. Reglas de privacidad más estrictas para las comunicaciones electrónicas.

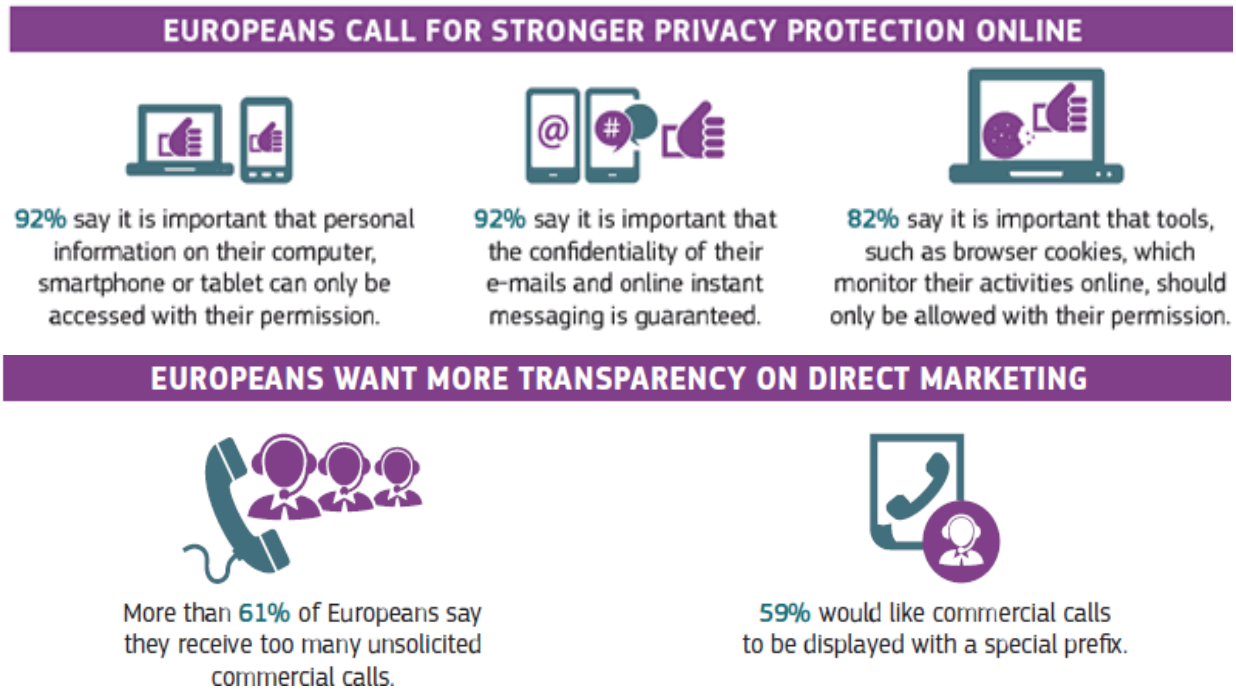
Como hemos visto antes, cada vez más europeos utilizan los servicios de comunicación en línea y con el ePR. Las comunicaciones electrónicas europeas son

confidenciales independientemente de la tecnología utilizada, las reglas propuestas también se aplicarán a los servicios de voz y mensajería por Internet.

En la siguiente figura, podemos observar que los europeos necesitan una mayor protección de la privacidad en línea, especialmente en sus dispositivos móviles (ordenador, teléfono inteligente o tableta).

Además, los europeos quieren más transparencia en el marketing directo. Debido a eso, con esta regulación, las personas tendrán que estar de acuerdo antes de que los mensajes de marketing sean enviados a ellos por máquinas de llamadas automáticas, SMS o correo electrónico, por ejemplo. También deberán aceptar recibir llamadas de marketing, a menos que la legislación nacional les otorgue el derecho de oponerse a la recepción de tales llamadas. Además, las personas que llaman de marketing deberán mostrar su número de teléfono o utilizar un pre-arreglo especial que indique una llamada de marketing.

Figura 10 - Protección de la privacidad online



Fuente: European Commission (2017)

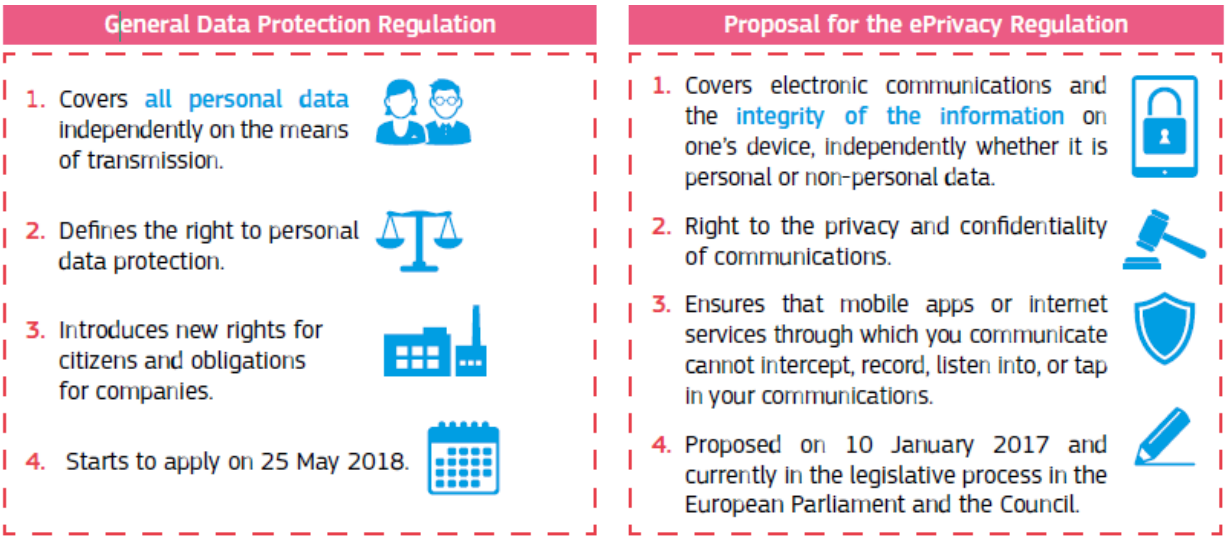
3.3. Ley aplicable y situaciones transfronterizas

La directiva sobre privacidad electrónica no contiene una disposición explícita con respecto a la legislación nacional aplicable. Esto puede crear incertidumbre legal sobre qué ley debería aplicarse en un contexto transfronterizo. La situación poco clara se deriva de la falta de una norma específica de ley aplicable, lo que dificulta una aplicación efectiva de las normas en una situación transfronteriza.

3.4. Relación entre el GDPR y ePR

Existen pocas diferencias y similitudes con respecto al GDPR y al ePR. Mientras que el ePR protege la confidencialidad de las comunicaciones electrónicas, el GDPR protege los datos personales. Esto significa que el ePR complementa el GDPR en el sector de las comunicaciones electrónicas. En la siguiente figura tenemos una comparación entre el GDPR y el ePR.

Figura 11 - GDPR vs ePR

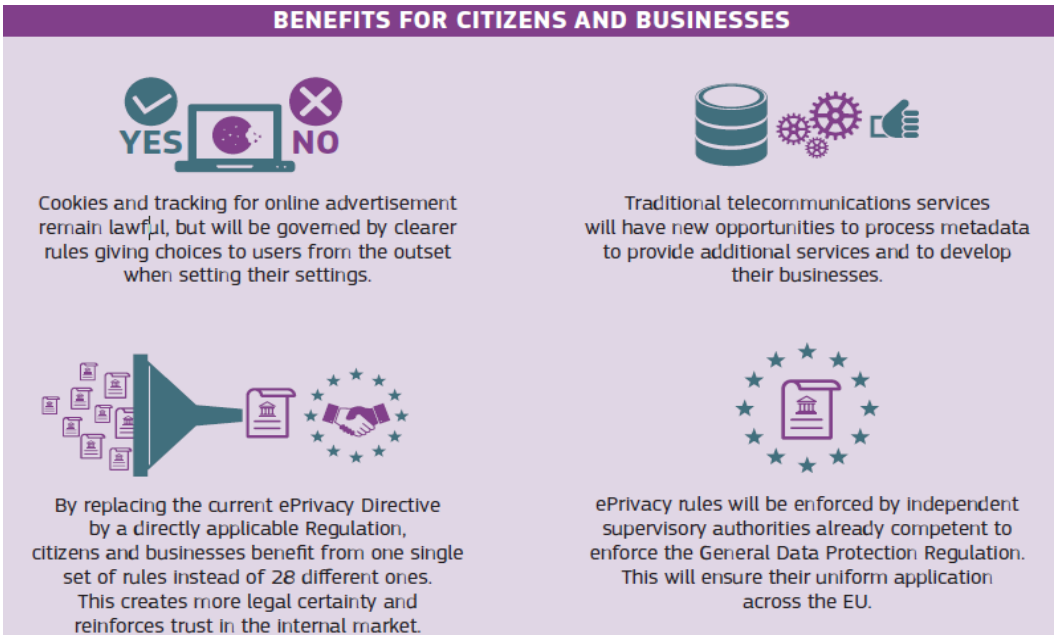


Fuente: European Commission (2016)

3.5. Beneficios para ciudadanos y empresas

Según la Comisión Europea, este reglamento tiene algunos beneficios para los ciudadanos y las empresas. Los principales beneficios para los ciudadanos y las empresas se pueden ver en la siguiente figura.

Figura 12 - Benecios para ciudadanos y empresas



Fuente: European Commission (2017)

4. Protección de datos personales

Según la Comisión Europea, los datos personales son cualquier información relacionada con un individuo vivo identificado o identificable. En otras palabras, los datos personales son cualquier información que pueda usarse para identificar a una persona.

El marco de protección de datos y privacidad de la UE tiene dos regulaciones principales: GDPR y ePR.

El GDPR 2016/679 es un reglamento de la UE sobre protección de datos y privacidad para todos los ciudadanos de la UE y también del EEE.

El GDPR entró en vigencia el 25 de mayo de 2018 en cada país europeo. El objetivo del GDPR es imponer una ley uniforme de seguridad de datos a todos los miembros de la UE para que cada estado miembro ya no necesite redactar sus propias leyes de protección de datos y, como consecuencia, las leyes sean consistentes en toda la UE. Los requisitos del GDPR tienen como objetivo crear una protección más consistente de los datos personales y del consumidor en todos los países de la UE.

Además, GDPR se enfoca en garantizar que los usuarios conozcan, comprendan y den su consentimiento a los datos recopilados sobre ellos. El RGPD protege los datos personales independientemente de la tecnología (procesamiento automatizado o manual) utilizada para procesar esos datos de acuerdo con criterios predefinidos. Además, no importa cómo se almacenen los datos (por ejemplo, video, papel, etc.), en todos los casos, los datos personales están sujetos a los requisitos de protección establecidos por el GDPR y el ePR.

El ePR tiene como objetivo proporcionar un alto nivel de protección de la privacidad para los usuarios de servicios de comunicaciones electrónicas y fue propuesto por la Comisión Europea en enero de 2017 como parte de su estrategia de mercado único digital y reemplazará la directiva de privacidad electrónica de 2002.

Aunque el reglamento básico de protección de datos es directamente aplicable como reglamento de la UE en cada estado miembro de la UE, contiene algunas cláusulas de apertura y deja al legislador nacional un margen de maniobra, como veremos en la siguiente sección.

4.1. ¿Qué regulaciones complementan las regulaciones europeas?

4.1.1. Austria

Las normas aplicadas en materia de protección de datos personales son:

- **GDPR** - en **alemán Datenschutz-Grundverordung (DSVGO);**
- **ePR**;
- **Ley de Protección de Datos de Austria Datenschutzgesetz (DSG)** que complementa el RGPD;
- **La Ley de adaptación de protección de datos de 2018 y la Ley de desregulación de protección de datos de 2018** (dos enmiendas a la Ley de protección de datos) se adoptaron para implementar estas cláusulas de apertura y márgenes. La Ley de adaptación de protección de datos de 2018 se publicó en BGBl

I No. 120/2017 y la Ley de desregulación de protección de datos de 2018 en BGBl I No. 24/2018 entraron en vigor el 25 de mayo de 2018;

- **La directiva de protección de datos** es una directiva para el área de Justicia y asuntos de Interior basada en la directiva basada en la Directiva de la UE (UE) 2016/680 del Parlamento Europeo y del Consejo del 27 de abril de 2016 sobre la protección de las personas con respecto al procesamiento de datos personales por parte de las autoridades competentes para los siguientes propósitos: prevención, investigación, detección o enjuiciamiento de delitos, ejecución de sentencias, sobre la libre circulación de datos y derogación de la Decisión Marco 2008/977 / JAI del Consejo (Österreichische Datenschutzbehörde, 2019).

4.1.2. República Checa

En el caso de la República Checa, la legislación aplicable es la siguiente:

- **GDPR;**
- **ePR**;
- **La Resolución No. 205** (15 de marzo de 2010) aborda los problemas de seguridad cibernética y ha establecido el Ministerio del Interior de la República Checa como coordinador de los problemas de seguridad cibernética y la autoridad nacional para el área;
- **La Resolución No. 380** (24 de mayo de 2010) estableció el Consejo de Coordinación Interdepartamental para el área de seguridad cibernética;
- **La Resolución No. 564** (20 de julio de 2011) está relacionada con la Estrategia de Ciberseguridad checa para el período 2011-2015;
- **La Resolución No. 781** (19 de octubre de 2011) estableció a la Autoridad como coordinadora de los asuntos de seguridad cibernética, así como la autoridad nacional para el área de seguridad cibernética;
- **La Ley de Ciberseguridad** (1 de enero de 2015) está directamente relacionada con los problemas de ciberseguridad;
- **El Decreto no 437/2017** (8 de diciembre de 2017) transpone la legislación pertinente de la UE y regula los criterios sectoriales y de impacto para la

determinación de un operador de servicio esencial y las especificaciones para determinar la importancia de un impacto de la interrupción de un servicio esencial en el seguridad de las actividades sociales y económicas;

- **La Ley No 181/2014 Coll** (19 de diciembre de 2014) sobre seguridad cibernética y el cambio de actos relacionados se publicaron en la Colección de Leyes: Decreto No 316/2014 Coll. sobre medidas de seguridad, incidentes de ciberseguridad y medidas reactivas ("Reglamento de ciberseguridad"); Decreto no 317/2014 Coll. sobre sistemas de información importantes y sus criterios de determinación; y, orden gubernamental no 315/2014 Coll. que modifica la orden gubernamental no 315/2014 Coll. que modifica la orden gubernamental no 432/2010 Coll. sobre los criterios para la identificación de un elemento de infraestructura crítica;

- **El Decreto No 82/2018 Coll** (21 de mayo de 2018) está relacionado con medidas de seguridad, incidentes de ciberseguridad, medidas reactivas, requisitos de informes de ciberseguridad y eliminación de datos (el Decreto de Ciberseguridad).

4.1.3. Portugal

En Portugal, el marco de protección de datos personales está regulado por:

- **GDPR**;
- **ePR**;
- **Ley de privacidad electrónica** (29 de agosto de 2012) que debe aplicarse al procesamiento de datos personales en relación con la provisión de servicios públicos de comunicaciones electrónicas disponibles en redes de comunicaciones públicas, incluidas las redes de comunicaciones públicas que admiten dispositivos de recopilación e identificación de datos, especificando y complementando las disposiciones de Ley nº 67/98 de 26 de octubre. Las empresas que prestan servicios de comunicaciones electrónicas disponibles al público deben establecer procedimientos internos para responder a las solicitudes de acceso a los datos personales del usuario presentados por las autoridades judiciales competentes de

conformidad con la legislación especial mencionada. Según la Ley de privacidad electrónica, la entrega de comunicaciones no solicitadas para marketing directo está sujeta al consentimiento previo del suscriptor que es un individuo o el usuario;

- Constitución de la República Portuguesa (artículo 35) que establece que todos los ciudadanos tienen el derecho de acceso a los datos informatizados relacionados con ellos y el derecho a ser informados sobre el uso para el que están destinados los datos. Por lo tanto, según esta ley, tienen derecho a exigir que el contenido de los archivos y registros se corrija y actualice. Esta ley determina qué datos personales son, así como las condiciones aplicables al procesamiento, conexión, transmisión y uso automáticos y debe garantizar su protección por medio de un organismo administrativo independiente;

- **Ley de Protección de Datos - Ley 67/98** - (26 de octubre de 1998), que es el marco legal que generalmente se aplica a los sectores público y privado, así como a cualquier actividad del sector. La Ley de Protección de Datos tiene como objetivo proteger el derecho de una persona a la vida privada mientras procesa datos personales estableciendo los derechos y procedimientos asociados de personas físicas (sujetos de datos) y los derechos, deberes y responsabilidades de las personas jurídicas y físicas al procesar datos personales. La Ley de Protección de Datos también establece los principios y obligaciones que aquellos que manejan los datos deben cumplir al realizar el procesamiento de datos personales. El principio general de esta ley establece que el procesamiento de datos personales se llevará a cabo de manera transparente y estricta para la privacidad y otros derechos, libertades y garantías fundamentales;

- Ley 32/2008 (18 de julio de 2008) que establece las obligaciones de retención de datos impuestas a los proveedores de servicios de comunicaciones electrónicas disponibles. Esta ley está relacionada con la retención de datos generados o procesados en relación con la provisión de servicios públicos de comunicaciones electrónicas disponibles o redes públicas de comunicaciones;

- **Leyes de comunicación electrónica - Ley 5/2014** - (10 de febrero de 2004) y la **Ley de privacidad electrónica.** Según estas leyes, en caso de una violación

de seguridad o integridad, estos proveedores deben notificar al regulador (la Autoridad Nacional de Comunicaciones o ANACOM), la Comisión Nacional de Protección de Datos y, en algunas circunstancias, los suscriptores y usuarios del servicio;

- **Directiva de la UE 2016/1148** sobre seguridad cibernética. Según esta directiva, existen medidas para un alto nivel común de seguridad de redes y sistemas de información en toda la UE en julio de 2016. Esta directiva permite la extensión a otras entidades de la obligación de implementar medidas de seguridad y notificar las violaciones de seguridad.

4.1.4. España

En España, la legislación de protección de datos personales que se aplica es la siguiente:

- **GDPR**;
- **ePR**;
- **El Tratado de Lisboa (la carta de derechos fundamentales de la UE) y la Constitución española de 1978** que están relacionadas con la protección de datos y la privacidad y son derechos fundamentales;
- **Varios códigos de conducta para la protección de datos** que fueron aprobados bajo las antiguas regulaciones españolas de protección de datos para diversos sectores;
- **Las regulaciones específicas del sector** que también incluyen disposiciones de protección de datos ya que ciertas categorías de datos personales y ciertas actividades de procesamiento pueden requerir protección específica como el procesamiento de datos personales dentro de los sectores financieros, de comunicaciones electrónicas o relacionados con la salud;
- **La nueva Ley Española de Protección de Datos** (25 de mayo de 2018) proporciona una regulación específica de protección de datos en diferentes campos que no están expresamente incluidos en el GDPR o que están incluidos en el GDPR pero con un alcance que permitió que los estados miembros introdujeran

regulaciones más detalladas. Además, esta ley incorpora al sistema legal español una lista de los nuevos derechos de los ciudadanos en relación con las nuevas tecnologías conocidas como "derechos digitales". Esta ley también incluye una enmienda de la Ley Electoral General española, que permite a los partidos políticos procesar datos personales para actividades específicas de promoción electoral;

- **La Ley de Comercio Electrónico 34/2002 (LSSI)** y la **Ley General de Telecomunicaciones 9/2014 (GT**L) que están relacionadas con las especificaciones específicas del sector también pueden contener disposiciones de protección de datos;

- **Directiva UE 2016/680** (27 de abril de 2016) del Parlamento Europeo y del Consejo, del 27 de abril de 2016, sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes a efectos de prevención, investigación, detección o enjuiciamiento de delitos o la ejecución de sanciones penales, y sobre la libre circulación de dichos datos, y derogando la Decisión Marco 2008/977 / JAI del Consejo;

- **Código de ciberseguridad** que reúne todas las reglas actualizadas que afectan directamente a la ciberseguridad. Sin embargo, las regulaciones de ciberseguridad aún necesitan un mayor desarrollo.

En la siguiente tabla, encontrará un breve resumen de las leyes de protección de datos personales que se aplican en República Checa, Portugal y España.

Tabla 1 - Legislación de protección de datos personales

	Datos personales		Datos no personales	Legislación adicional de datos personales	Breve explicación
	GDPR	ePR	Regulación (UE 2018/1807)		
Austria	✓	✓	✓	**Ley de protección de datos austriaca Datenschutzgesetz**	La Ley de protección de datos de Austria (DSG) complementa el GDPR
				Ley de Adaptación de Protección de Datos de 2018 (BGBI I No. 120/2017)	Estas dos leyes fueron adoptadas para implementar las cláusulas de apertura y los márgenes (además de las enmiendas a numerosas leyes materiales) a la Ley de Protección de Datos. Además, estas leyes complementan el GDPR
				Ley de desregulación de protección de datos de 2018 (BGBI I No. 24/2018)	
				Directiva de protección de datos	La presente Directiva se basa en la Directiva de la UE 2016/680 del Parlamento Europeo y del Consejo, del 27 de abril de 2016, sobre la protección de las personas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes a efectos de prevención, investigación , detección o enjuiciamiento de delitos penales o de ejecución de sentencias, sobre la libre circulación de datos
Czech Republic	✓	✓	✓	**Resolución No. 205**	Abordar los problemas de seguridad cibernética y estableció el Ministerio del Interior de la República Checa como coordinador de los problemas de seguridad cibernética y la autoridad nacional para el área.
				Resolución No. 380	Estableció el Consejo de Coordinación Interdepartamental para el área de seguridad cibernética.
				Resolución No. 564	Estrategia checa de ciberseguridad 2011-2015
				Resolución No. 781	Autoridad como coordinador de asuntos de ciberseguridad, así como a nivel nacional.

				Ley de ciberseguridad	Esta ley regula la ciberseguridad en la República Checa y está vigente desde el 1 de enero de 2015.
				Decreto no 437/2017	Este decreto transpone la legislación pertinente de la UE y regula los criterios sectoriales y de impacto para la determinación de un operador de servicios esenciales y las especificaciones para determinar la importancia de un impacto de la interrupción de un servicio esencial en la seguridad de las actividades sociales y económicas.
				Ley no 181/2014 Coll	Relacionado con la ciberseguridad y el cambio de actos relacionados con este tema
				Decreto no 82/2018 Coll	Conectado a medidas de seguridad, incidentes de ciberseguridad, medidas reactivas, requisitos de informes de ciberseguridad y eliminación de datos (el Decreto de Ciberseguridad
Portugal	✓	✓	✓	**Ley de privacidad electrónica**	Procesamiento de datos personales en relación con la provisión de servicios públicos de comunicaciones electrónicas disponibles en redes públicas de comunicaciones, incluidas las redes públicas de comunicaciones que admiten dispositivos de identificación y recolección de datos
				Constitución de la República portuguesa (artículo 35)	Establezca que todos los ciudadanos tienen el derecho de acceso a cualquier información computarizada relacionada con ellos y el derecho a ser informados sobre el uso para el que están destinados los datos, por lo tanto, bajo esta ley, tienen derecho a exigir que el contenido de los archivos y los registros deben ser corregidos y actualizados. Esta ley determina qué datos personales son, así como las condiciones aplicables al procesamiento, conexión, transmisión y uso automáticos y debe garantizar su protección por medio de un organismo administrativo independiente
				Ley 67/98 de 26 de octubre.	Marco legal sobre la ley de protección de datos que generalmente se aplica a los sectores público y privado, así como a cualquier actividad del sector.
				Ley 32/2008 del 18 de julio	Establece las obligaciones de retención de datos impuestas a los proveedores de servicios de comunicaciones electrónicas disponibles al público.

				Ley 5/2014 de 10 de febrero y Ley de privacidad electrónica	Según estas leyes, en caso de incumplimiento de seguridad o integridad, estos proveedores deben notificar al regulador (la Autoridad Nacional de Comunicaciones o ANACOM), la Comisión Nacional de Protección de Datos y, en algunas circunstancias, los suscriptores y usuarios del servicio.
				Directiva de la UE 2016/1148	Permite la extensión a otras entidades de la obligación de implementar medidas de seguridad y notificar violaciones de seguridad
Spain	✓	✓	✓	**Tratado de Lisboa Constitución española de 1978**	Están relacionadas con la protección de datos y la privacidad, y son derechos fundamentales.
				Nueva Ley Española de Protección de Datos Ley 3/2018 del 7 de diciembre	Proporcionar regulación de protección de datos específica en diferentes campos que no están expresamente incluidos en el GDPR o que están incluidos en el GDPR pero con un alcance que permitió que los estados miembros introdujeran regulaciones más detalladas
				Ley de comercio electrónico 34/2002 (LSSI) **Ley General de Telecomunicaciones 9/2014 (GTL)**	Relacionado con regulaciones específicas del sector
				Directiva UE 2016/680 del Parlamento Europeo y del Consejo del 27 de abril de 2016	Protección de las personas físicas con respecto al procesamiento de datos personales por parte de las autoridades competentes a los efectos de la prevención, investigación, detección o enjuiciamiento de delitos o la ejecución de sanciones penales y sobre la libre circulación de dichos datos, y derogar la Decisión Marco del Consejo 2008/977 / JAI
				Código de ciberseguridad	Establece las principales reglas que deben tenerse en cuenta con respecto a la protección del ciberespacio y para garantizar la ciberseguridad antes mencionada.

Fuente Elaboración propia del autor.

5. Datos no personales

El flujo libre de datos no personales se traduce en el movimiento sin restricciones de datos a través de la frontera y los sistemas de tecnología de la información en la UE.

La normativa sobre el libre flujo de datos no personales en la UE ya está en vigor. El nombre exacto de este reglamento es el reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, del 14 de noviembre de 2018, sobre un marco para el libre flujo de datos no personales en la UE.

Este reglamento tiene como objetivo garantizar el libre flujo de datos que no sean datos personales dentro de la UE mediante el establecimiento de normas relativas a los requisitos de localización de datos, la disponibilidad de datos a las autoridades competentes y la portabilidad de datos para usuarios profesionales.

Este reglamento también se aplica al procesamiento de datos electrónicos que no sean datos personales en la UE, que es:

- Proporcionado como un servicio a usuarios que residen o tienen un establecimiento en la Unión, independientemente de si el proveedor de servicios está establecido o no en la Unión;
- Llevado a cabo por una persona jurídica o de datos que resida o tenga un establecimiento en la Unión para sus propias necesidades;

Este reglamento no se aplica a una actividad que queda fuera del ámbito de aplicación del Derecho de la Unión.

Figura 13 - Datos no personales

Fuente: Business2Community (2019)

La garantía del libre flujo de datos no personales tiene los siguientes principios en toda la UE:

- El principio del libre flujo de datos no personales elimina las restricciones injustificadas de localización de datos impuestas por las autoridades públicas, lo que aumenta la seguridad jurídica y aumenta la confianza;
- El principio de disponibilidad de datos para las autoridades competentes asegura que los datos permanezcan accesibles para el control regulatorio y de supervisión también cuando se almacenan o procesan a través de las fronteras en la UE;
- Acciones para alentar a los proveedores de servicios en la nube a desarrollar códigos de conducta autorreguladores para facilitar el cambio de proveedor y transferir los datos a los servidores internos, que deben implementarse a mediados de 2020;
- Los requisitos de seguridad en el almacenamiento y procesamiento de datos siguen siendo aplicables, también cuando las empresas almacenan o procesan datos en otro estado miembro. Lo mismo se aplica cuando subcontratan el procesamiento de datos a proveedores de servicios en la nube;
- Puntos de contacto únicos en cada estado miembro para establecer enlaces con los puntos de contacto de otros estados miembros y la comisión para garantizar la aplicación efectiva de las nuevas reglas sobre el libre flujo de datos no personales.

El **GDPR y la regulación sobre el flujo libre de datos no personales funcionarán juntos para permitir el flujo libre de cualquier dato**, creando un espacio europeo común para los datos. Estas dos regulaciones juntas crean seguridad jurídica para las empresas y garantizan que los datos personales y no personales puedan moverse libremente dentro de la UE.

5.1. Libre circulación de datos dentro de la UE

Los requisitos de localización de datos estarán prohibidos a menos que estén justificados por razones de seguridad pública de conformidad con el principio de proporcionalidad. Por lo tanto, los estados miembros comunican inmediatamente a la comisión cualquier proyecto de ley que introduzca un nuevo requisito de localización de datos o realice

cambios en un requisito de localización de datos existente de acuerdo con los procedimientos presentes en los artículos 5, 6 y 7 de la Directiva (UE) 2015/1535 .
Además, la **regulación aplicada a los datos no personales** garantiza:
- **Libre circulación de datos no personales a través de las fronteras:** todas las organizaciones deberían poder almacenar y procesar datos en cualquier lugar de la UE;
- **La disponibilidad de datos para el control reglamentario:** las autoridades públicas mantendrán el acceso a los datos, también cuando estén ubicados en otro estado miembro o cuando estén almacenados o procesados en la nube;
- Cambio más fácil de proveedores de servicios en la nube para usuarios profesionales. La Comisión ha comenzado a facilitar la autorregulación en esta área, alentando a los proveedores a desarrollar códigos de conducta con respecto a las condiciones bajo las cuales los usuarios pueden transferir datos entre proveedores de servicios en la nube y volver a sus propios entornos de TI;
- Total consistencia y sinergias con el paquete de seguridad cibernética y aclaración de que los requisitos de seguridad que ya se aplican a las empresas que almacenan y procesan datos continuarán haciéndolo cuando almacenen o procesen datos a través de las fronteras en la UE o en la nube.

Junto con esta regulación, el GDPR ya prevé la libre circulación de datos personales. Para el 30 de mayo de 2021, los estados miembros tienen algunas reglas con respecto a los requisitos de localización de datos establecidos sobre la base de la legislación vigente de la Unión.

5.2. Porting of data

The European Commission shall encourage and facilitate the development of self-regulatory codes of conduct at Union level in order to contribute to a competitive data economy, based on the principles of transparency and facilitate the development of self-regulatory codes in order to contribute to a competitive data economy.

5.3. Procedure for cooperation between authorities

According to article 7, each member state shall designate a single point of contact which shall liaise with the single points of contact with the others member states and the Commission regarding the application of this regulation. This means that member states shall notify to the Commission the designated single points of contact and any subsequent change.

5.4. Disponibilidad de datos para autoridades competentes

En lo que respecta al artículo número 5, el presente Reglamento no afectará a las facultades de las autoridades competentes para solicitar u obtener acceso a los datos para el desempeño de sus funciones oficiales de conformidad con la legislación de la Unión o nacional. Después de solicitar acceso a los datos de un usuario, una autoridad competente no obtiene acceso y, si no existe un mecanismo de cooperación específico de conformidad con la legislación de la Unión o los acuerdos internacionales para intercambiar datos entre las autoridades competentes de diferentes estados miembros, esa autoridad competente puede solicitar asistencia de una autoridad competente en otro estado miembro de conformidad con el artículo 7.

5.5. Sanciones por infracciones

Este reglamento establece sanciones por una infracción que describe diferentes sanciones por diferentes infracciones (las mismas sanciones que se aplican bajo GDPR también se aplican al ePR). Esto significa que las sanciones oscilan entre 10 millones de euros o el 2% de la facturación anual mundial por infracciones más graves, la que sea mayor en cada caso.

Las eventuales multas dependen en gran medida de una serie de factores atenuantes, como la escala del incidente, si se produjo una violación de la regulación como resultado de un acto deliberado y cuán diligente fue la empresa con respecto a la prevención de tales incidentes.

6. Catálogo de contenido sistematizado

Ciberseguridad: es la práctica de proteger sistemas, redes y programas de ataques digitales. Estos ataques cibernéticos generalmente tienen como objetivo acceder, cambiar o destruir información confidencial, extorsionar a los usuarios o interrumpir los procesos comerciales normales.

Ley de protección de datos: autoridades públicas independientes que supervisan la aplicación de la ley de protección de datos. Brindan asesoramiento experto sobre temas de protección de datos y manejan quejas contra violaciones del GDPR y las leyes nacionales relevantes.

Oficial de protección de datos: la persona responsable del monitoreo y la aplicación de las normas de protección de datos en la Comisión Europea. Un DPO es un empleado dentro de su organización que es responsable de comprender y garantizar el cumplimiento de su organización. El DPO garantiza la aplicación interna de las normas de protección de datos en cooperación con el Supervisor Europeo de Protección de Datos.

Reglamento de privacidad electrónica: propuesta de la Comisión Europea diseñada para fortalecer la protección de la vida privada de los ciudadanos de la Unión Europea y crear nuevas oportunidades para los negocios.

GDPR: regulación en la legislación de la UE sobre protección de datos y privacidad para todos los ciudadanos individuales de la Unión Europea y el Espacio Económico Europeo. También aborda la transferencia de datos personales fuera de la Unión Europea y el Espacio Económico Europeo.

Datos no personales: información electrónica que no se puede rastrear hasta una persona física identificada o identificable (o que ha sido anonimizada como tal).

Datos personales: cualquier información relacionada con un individuo que pueda identificarse directa o indirectamente. Nombres, fotos, información geográfica, cookies web, dirección de correo electrónico son algunos ejemplos de datos personales.

7. Conclusiones

La protección de datos y la ciberseguridad se están convirtiendo en valores esenciales para la sociedad y, por eso, estas dos áreas han experimentado un desarrollo legal significativo y están más consolidadas en la UE.

La regulación para el tratamiento de datos personales difiere de la regulación para los datos no personales en los estados miembros de la UE. Sin embargo, las regulaciones que conciernen a los datos no personales y personales son las mismas para todos los estados miembros. En este contexto, la regulación (UE) 2018/1807 se aplica al libre flujo de personas no personales, mientras que con respecto a la protección de datos, como en todas las demás jurisdicciones de la UE, la regla principal es el GDPR. Junto con el GDPR, la regulación relacionada con el flujo libre de datos no personales funcionará en conjunto para permitir el flujo libre de cualquier dato que resulte en un espacio europeo común para datos.

Además, el ePR establece algunas reglas relacionadas con la protección de la privacidad en el sector de las comunicaciones electrónicas. En particular, esta regulación se aplica a los proveedores de redes y servicios de comunicaciones electrónicas y debía entrar en vigencia el 25 de mayo de 2018, junto con el GDPR, sin embargo, la continua deliberación y el cabildeo de algunos de sus mejores han retrasado la aplicación de esta regulación. El ePR no contiene una disposición explícita con respecto a la ley nacional aplicable que crea inseguridad jurídica sobre qué ley debería aplicarse en un contexto transfronterizo.

Sin embargo, aunque la regulación básica de protección de datos es directamente aplicable como una regulación de la UE en cada estado miembro de la UE, contiene numerosas cláusulas de apertura y deja margen de maniobra al legislador nacional.

8. Referencias

Business2Community (2019). Why User Data is the Next Big Deal in Digital? Retrieved from https://www.business2community.com/mobile-apps/why-user-data-is-the-next-big-deal-in-digital-02179282.

Deloitte (2019). The GDPR: Six Months after Implementation. Retrieved from https://www2.deloitte.com/bg/en/pages/legal/articles/gdpr-six-months-after-implementation-2018.html.

EU GDPR.ORG (2019). The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years. Retrieved from https://eugdpr.org/.

European Commission (2019). Complete guide to GDPR compliance. Retrieved from https://gdpr.eu/.

European Commission (2019). Data protection under GDPR. Retrieved from https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_en.htm#shortcut-3-who-monitors-how-personal-data-is-processed-within-a-company.

European Commission (2019). Eurobarometer on ePrivacy. Retrieved from https://ec.europa.eu/digital-single-market/en/news/eurobarometer-eprivacy.

European Commission (2019). Free flow of non-personal data. Retrieved from https://ec.europa.eu/digital-single-market/en/free-flow-non-personal-data.

European Commission (2019). General Data Protection Regulation: one year on. Retrieved from: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2610.

European Commission (2019). Proposal for a regulation on privacy and electronic communications. Retrieved from https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications.

i-Scoop (2019). Data processing principles: the 9 GDPR principles relating to processing personal data. Retrieved from https://www.i-scoop.eu/gdpr/gdpr-personal-data-processing-principles/.

ITPRO (2019). ePrivacy Regulation: What is it and how does it affect me? Retrieved from https://www.itpro.co.uk/privacy/32712/eprivacy-regulation-what-is-it-and-how-does-it-affect-me.

Serve IT (2017). GDPR for developers - data subject rights. Retrieved from https://www.serveit.com/gdpr-for-developers-data-subject-rights/.