Ley de protección de datos

Guía

Versión: 1.0

Revisado: Enero 2024

Contenido

Resumen 3

Fundamentos 4

- Datos protegidos 4
- Principales actores 5
- Elementos de Derecho 6

Requisitos 7

- Derechos de los consumidores 8
  - Opt-Out 8
  - Uso y modificación de datos 8
- Obligaciones del interventor 10
  - Protección de datos 10
  - Consentimiento del consumidor 12
  - Finalidad Limitaciones 13
  - DPIA 14

Leyes 15

- GDPR 16
- Estados Unidos 17
- Otros 20
  - Canadá 20
  - India 20
  - México 21

Recursos 22

Glosario 23

Resumen

Las leyes sobre privacidad de datos proliferan rápidamente en todo el mundo. A medida que el número de violaciones de datos se ha disparado y los consumidores son cada vez más conscientes e inteligentes, los gobiernos han respondido promulgando nuevas y estrictas normativas que regulan cómo se recopilan, procesan, almacenan y venden los datos en línea.

Es poco probable que esta tendencia ceda. El éxito de leyes históricas como el Reglamento General de Protección de Datos (RGPD) en Europa y otras leyes recientes han creado un efecto de bola de nieve en el que las jurisdicciones se basan cada vez más en el progreso de otras, lo que resulta en un movimiento acelerado hacia normas de privacidad de datos amplias y de gran alcance. Para 2025, se prevé que el 75 % de la población mundial estará cubierta por normativas de privacidad modernas.

Para los hoteleros, el creciente alcance y rigor de la legislación sobre privacidad de datos añade una complejidad sin precedentes a un juego de cumplimiento normativo en el que ya hay mucho en juego. Las organizaciones que tratan de evitar los costes financieros potencialmente enormes y el daño a la reputación que puede suponer el incumplimiento de la normativa tendrán que enfrentarse ahora a múltiples conjuntos legislativos que se solapan (y pueden entrar en conflicto).

Ante este panorama, los hoteleros con visión de futuro deben dar prioridad a la educación y la concienciación. Aunque es prudente confiar en un asesor cualificado para resolver ciertas cuestiones jurídicas, también incumbe a los líderes de la organización tener una comprensión básica de los preceptos de la ley de privacidad de datos, ser conscientes del terreno normativo en el que operan y actuar en consecuencia para establecer culturas sólidas de privacidad y seguridad de datos en sus equipos.

Para ello, esta guía introduce y analiza los conceptos, requisitos y leyes fundamentales relacionados con la privacidad de los datos.

Fundamentos

Para los recién llegados a este campo, la legislación sobre privacidad de datos puede parecer inabordable y abrumadora. Debido a su impacto expansivo y a su terminología legalista, a menudo se ha dejado de lado o se ha encomendado únicamente a especialistas y abogados.

No tiene por qué ser así.

Las leyes de privacidad, en su esencia, se rigen por principios que son a la vez lógicos y sencillos.

Para entenderlas, sin embargo, es necesario operar con una serie de conocimientos básicos y fundamentales. Los siguientes conceptos son esenciales para comprender el significado de estas leyes.

Datos protegidos

La legislación sobre privacidad se centra en la protección de determinados tipos de datos que pueden utilizarse para identificar, contactar, localizar o inferir información sobre un individuo, ya sea directa o indirectamente, con el fin de salvaguardar los derechos de los individuos a la privacidad y autonomía de su información personal.

Lo más habitual es que este tipo de datos resida en una categoría de información que se denomina *datos personales*.

Tal como se define en el GDPR, "datos personales" incluye cualquier información relativa a una persona física identificada o identificable. Algunos ejemplos son los siguientes:

Identificadores Nombres, números de identificación, SSN, etc.	**Información de contacto** Direcciones o números de teléfono.	**Demografía** Edad, sexo, etnia, etc.
Información financiera Números de tarjetas de crédito, cuentas bancarias, ingresos, etc.	**Datos sanitarios** Historiales médicos, información sobre seguros, datos genéticos.	**Datos de empleo** Historial laboral o evaluaciones.

Información educativa Expedientes académicos, certificaciones o registros de formación.	**Identificadores en línea** Direcciones IP, cookies o etiquetas RFID.	**Datos de localización** Datos GPS u otra información de geolocalización.

En Estados Unidos, históricamente se había utilizado con frecuencia el término más restringido de "información de identificación personal" (IIP). Sin embargo, con la creciente influencia de la norma GDPR, las leyes estatales modernas han adoptado con frecuencia el lenguaje "datos personales".

Aunque la terminología de las leyes de protección de datos de todo el mundo puede ser muy variada, el concepto básico suele ser común: cada una de ellas se refiere a información relacionada con una persona que puede identificarla, ya sea por sí sola o en conjunción con otros datos.

Esta coherencia refleja una convergencia mundial hacia una comprensión más amplia e inclusiva de lo que constituye información identificable en la era digital.

Actores clave

La ley de protección de datos implica a varias partes interesadas con funciones, derechos y obligaciones únicos. Cada uno tiene una función distinta y la ley le afecta de manera diferente.

En el cuadro siguiente se desglosan las categorías habituales de actores y la forma típica en que les afecta la legislación sobre privacidad.

Categoría	Definición	Efecto jurídico
Sujeto de los datos	Persona física identificada o identificable cuyos datos personales son tratados por un responsable o un encargado del tratamiento. Nombre formal de un consumidor o usuario.	*Derechos*

Controlador de datos	Entidad que determina los fines y medios del tratamiento de datos personales. Nombre formal de la empresa o entidad recaudadora.	*Responsabilidades*
Procesador de datos	Entidad que trata datos personales por cuenta del responsable del tratamiento. El encargado del tratamiento actúa bajo las instrucciones del responsable del tratamiento. Por ejemplo, un proveedor de servicios en la nube o un proveedor de CRM.	*Responsabilidades*
Organismo regulador	Autoridades establecidas por las leyes de privacidad de datos para supervisar el cumplimiento y la aplicación. Por ejemplo, en virtud del RGPD, cada miembro de la UE tiene una Autoridad de Protección de Datos (APD) responsable de supervisar y hacer cumplir la normativa en su jurisdicción.	*Ninguno*

Elementos de Derecho

Cada ley de protección de datos contiene ciertos elementos comunes que definen su funcionamiento. Conocerlos le permitirá evaluar rápidamente la pertinencia y las implicaciones de las nuevas leyes para su organización.

En el cuadro que figura a continuación se enumeran estos elementos y se ofrece la definición de cada uno de ellos.

Elemento	Definición
Cronología	Fechas e hitos específicos dentro de la ley. Tenga en cuenta que la fecha de *promulgación* y la de *entrada en vigor* son distintas.
Derechos	Derechos o privilegios que la ley concede a los interesados.

Requisitos	Obligaciones impuestas por la ley a las entidades que tratan datos personales.
Mecanismo de aplicación	Procedimientos para abordar las infracciones y garantizar el cumplimiento. Por lo general, se trata de la aplicación gubernamental por parte de los organismos reguladores, pero también puede incluir un derecho de acción privado.
Sanciones	Sanciones o multas impuestas por incumplimiento. Esto puede incluir acciones disciplinarias, incluidos mandamientos judiciales o incluso cargos penales.

Requisitos

Las leyes de protección de datos imponen una serie de requisitos que alteran la forma en que se recogen, procesan y almacenan los datos personales.

Estos mandatos garantizan que los datos se manejen de forma que se respete la autonomía individual y se proteja contra el uso indebido. El objetivo de estas leyes no es ahogar la innovación ni impedir el flujo de información, sino inculcar una cultura de la privacidad acorde con el uso ético y las expectativas de la sociedad.

Sujetos de los datos
Particulares / Consumidores

Controladores de datos
Organizaciones / Empresas

Por lo general, los requisitos incluidos en estos reglamentos pueden dividirse en dos categorías principales. La primera categoría abarca los derechos concedidos a *los interesados*, las personas a las que pertenecen los datos. La segunda categoría delinea las obligaciones impuestas a *los responsables del tratamiento de datos*, las entidades que determinan la finalidad y los medios del tratamiento de datos personales.

Juntos, estos derechos y obligaciones forman los dos pilares sobre los que se asienta el edificio de la legislación sobre privacidad de datos.

En esta sección se ofrece una descripción detallada de cada tipo.

Derechos del consumidor

Muchas leyes de protección de datos conceden al consumidor derechos adicionales que aumentan su capacidad de controlar cómo se recogen o utilizan sus datos. Esta sección destaca algunos de los derechos más comunes y significativos de la legislación reciente.

Opt-Out

Los derechos de exclusión voluntaria de los interesados se refieren a las disposiciones de las leyes de protección de datos que permiten a las personas decidir que sus datos personales no se recopilen, utilicen o divulguen para determinados fines.

Este derecho es especialmente pertinente en contextos como el marketing directo, en el que los interesados tienen la opción de impedir que las organizaciones utilicen sus datos personales para enviarles material promocional.

Los derechos de exclusión voluntaria también pueden aplicarse a otras actividades de tratamiento de datos, como vender datos personales a terceros o compartirlos con fines de investigación.

Cuando los interesados ejercen su derecho de exclusión voluntaria, el responsable del tratamiento debe atender la solicitud en un plazo razonable y cesar las actividades específicas de tratamiento de datos para las que se solicitó la exclusión voluntaria.

La legislación sobre protección de datos puede obligar a las organizaciones a proporcionar mecanismos claros y sencillos para que los interesados ejerzan su derecho de exclusión voluntaria, exigiendo a menudo que la opción de exclusión voluntaria sea tan accesible y sencilla como el proceso de dar el consentimiento.

Uso y modificación de datos

Los derechos de uso y modificación se incluyen en muchas leyes de privacidad de datos como medio de garantizar que los individuos mantengan el control sobre su información personal.

Estas disposiciones -que incluyen derechos como el acceso, la rectificación y la supresión, entre otros- representan las vías centrales

a través de las cuales los interesados pueden ejercer soberanía sobre sus datos.

La aplicación de estos derechos marca un cambio hacia una mayor transparencia y capacidad de actuación de las personas en la gestión de sus datos personales.

Subraya la influencia del movimiento mundial hacia el reconocimiento de la importancia de los datos personales como extensión de la autonomía personal.

La siguiente tabla desglosa los derechos comunes de uso y modificación de datos, sus definiciones y su prevalencia en las leyes de privacidad modernas.

Derecha	Definición	Prevalencia
Acceda a	Derecho del interesado a obtener del responsable del tratamiento confirmación de si se están tratando datos personales que le conciernen y, en tal caso, acceso a los datos personales e información sobre su tratamiento.	*Generalizada*
Corrección	Derecho del interesado a que se rectifiquen los datos personales inexactos, o a que se completen si están incompletos.	*Generalizada*
Supresión	Derecho del interesado a que el responsable del tratamiento borre sus datos personales en determinadas circunstancias, como cuando los datos ya no son necesarios para los fines que fueron recogidos o cuando el interesado retira su consentimiento. También conocido como "derecho al olvido".	*Generalizada*

Objeción al tratamiento automatizado	Derecho a oponerse a las decisiones basadas únicamente en el tratamiento automatizado, incluida la elaboración de perfiles.	*Menos común*
Portabilidad	Derecho a transferir datos personales de un responsable del tratamiento a otro en un formato estructurado, de uso común y lectura mecánica.	*Aumentar*

Obligaciones del controlador

En virtud de la legislación sobre protección de datos, las obligaciones del responsable del tratamiento son el conjunto completo de deberes jurídicos y éticos que las entidades designadas como responsables del tratamiento asumen cuando determinan los fines y los medios del tratamiento de datos personales.

Estas responsabilidades se establecen para imponer la rendición de cuentas y garantizar que los responsables del tratamiento de datos actúen no sólo dentro de los límites de la legalidad, sino también respetando la intimidad y la autonomía de los interesados.

En esta sección se detallan los tipos de obligaciones más comunes e impactantes.

Avisos sobre protección de datos

Los avisos de privacidad son comunicaciones formales que informan a las personas sobre cómo una entidad recoge, procesa y gestiona sus datos personales.

Sirven para dar transparencia a las actividades de tratamiento de datos y articular las prácticas de privacidad del responsable del tratamiento en términos claros. Garantizan que las personas conozcan el tratamiento de sus datos personales y comprendan sus derechos en relación con ellos.

Las notificaciones pueden abarcar varios tipos diferentes de actividad. En el cuadro siguiente se detallan sus formas habituales y si se encuentran comúnmente en las normativas modernas sobre privacidad.

Tipo	Definición	Requisito común
Notificación de violación de datos	Envío a particulares y autoridades en caso de violación de datos que suponga un riesgo para los interesados.	✓
Notificación inferencial	Notificaciones sobre datos inferidos o derivados del análisis de los datos recogidos.	✗
Aviso inicial	Se facilitan en el momento en que se recogen los datos personales, detallando cómo y por qué se tratarán los datos.	✓
Aviso interno	Comunicaciones dentro de una organización sobre prácticas generales de tratamiento de datos no dirigidas específicamente a los interesados.	✗
Aviso actualizado	Se publica cuando se producen cambios significativos en las actividades o políticas de tratamiento de datos.	✓

Aviso sobre comercialización por terceros	Revelaciones específicas a particulares sobre el uso de sus datos para marketing de terceros cuando los datos no se han compartido con el comercializador.	✕

Consentimiento del consumidor

El requisito del consentimiento del consumidor es un elemento central en la mayoría de las leyes de privacidad de datos, sirviendo como piedra angular de la autonomía del usuario sobre la información personal.

El consentimiento se define como una indicación libre, específica, informada e inequívoca de la conformidad del interesado con el tratamiento de sus datos personales.

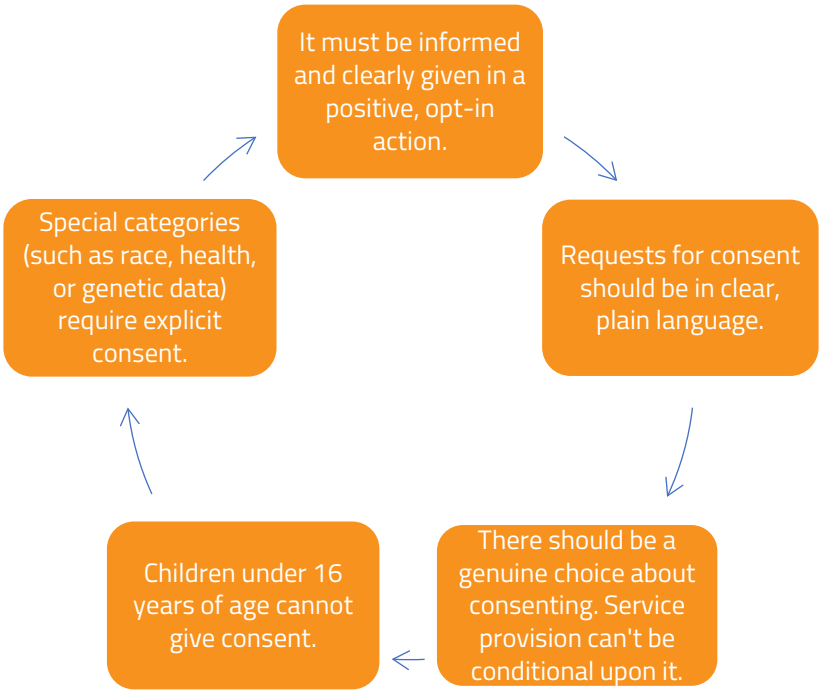
Esto significa que las personas deben poder elegir claramente si sus datos se utilizan y con qué fines, sin ser sometidas a ninguna forma de coacción, presión indebida o engaño.

Para que el consentimiento sea válido, debe darse mediante una acción afirmativa que signifique acuerdo, como marcar una casilla en un sitio web, elegir ajustes técnicos u otra declaración que indique claramente la aceptación del tratamiento propuesto de los datos personales. El silencio, las casillas marcadas previamente o la inactividad no suelen constituir un consentimiento válido con arreglo a regímenes estrictos de protección de datos como el RGPD.

Los interesados deben ser informados de forma adecuada y transparente sobre el alcance y las consecuencias del tratamiento de datos al que dan su consentimiento. Esto incluye quién recoge los datos, qué datos se recogen, cómo se utilizarán y si se compartirán con terceros.

Para las categorías sensibles de datos, que incluyen información sobre salud, raza, orientación sexual, creencias religiosas, etc., el requisito de consentimiento suele ser más estricto, necesitando un consentimiento explícito.

El requisito del consentimiento refleja el objetivo general de las leyes de privacidad de datos de otorgar a los individuos el control sobre sus datos personales, garantizando que las entidades que recogen y procesan datos lo hagan con el permiso explícito del individuo.



Criterios clave para el consentimiento del consumidor

Finalidad Limitaciones

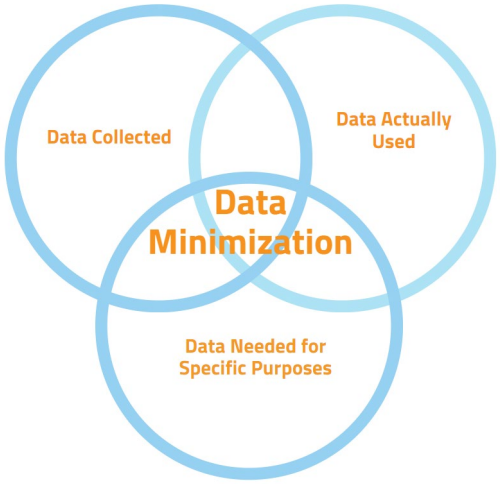
Además de requisitos precisos, muchas leyes de privacidad incluyen principios que sirven de orientación general para el comportamiento ético y legal. Un ejemplo de ello es el principio de "limitación a una finalidad específica", establecido por primera vez en el RGPD (artículo 5, apartado 1, letra b)).

En pocas palabras, este principio establece que:

> *'Los datos personales sólo deben recogerse con fines determinados, explícitos y legítimos, y no deben tratarse posteriormente de manera incompatible con dichos fines.'*

Este principio garantiza que las organizaciones sean transparentes sobre los motivos por los que tratan los datos y les impide utilizarlos para fines nuevos, no relacionados o ilícitos sin obtener el consentimiento del interesado o sin establecer otra base legítima conforme a la legislación aplicable.

La limitación de la finalidad ayuda a mantener la confianza de los interesados y preserva la integridad de las actividades de tratamiento de datos.



Minimización de datos visualizada

DPIA

Una Evaluación de Impacto sobre la Protección de Datos (EIPD) es un análisis sistemático y exhaustivo de cómo un proyecto o sistema concreto afectará a la privacidad de las personas implicadas.

La ley de protección de datos suele exigir la DPIA para ayudar a identificar y minimizar los riesgos de protección de datos de un proyecto.

Por ejemplo, las leyes pueden hacer obligatoria la EIPD cuando se produzcan determinados factores desencadenantes, como el tratamiento que implique una evaluación sistemática y amplia de aspectos personales basada en la toma de decisiones automatizada, el tratamiento a gran escala de datos sensibles, la vigilancia generalizada de zonas públicas u otros sucesos de alto riesgo.

Las EIPD funcionan como procesos normalizados. Su aplicación exacta puede variar, pero es útil entender que constan de cuatro fases:

Proceso de evaluación del impacto sobre la

- **Fase 1 - Preparación y planificación**

La fase inicial determina si es necesaria una EIPD, define su alcance y planifica cómo se llevará a cabo. Incluye la identificación de las actividades de tratamiento de datos y los fines para los que se tratan los datos personales.

- **Fase 2 - Evaluación de riesgos**

La segunda fase identifica y evalúa los riesgos potenciales para los derechos y libertades de los interesados que podrían derivarse de sus actividades. Esto incluye considerar la naturaleza, el alcance, el contexto y los fines del tratamiento, así como la probabilidad y gravedad de los riesgos.

- **Fase 3 - Desarrollo de estrategias de mitigación**

Basándose en la evaluación de riesgos, la tercera fase identifica las medidas que pueden mitigar los riesgos. Se trata de decidir las medidas que deben adoptarse para evitar o reducir el impacto de los riesgos detectados, garantizar la protección de los datos y cumplir la legislación aplicable.

- **Fase 4 - Documentación e integración**

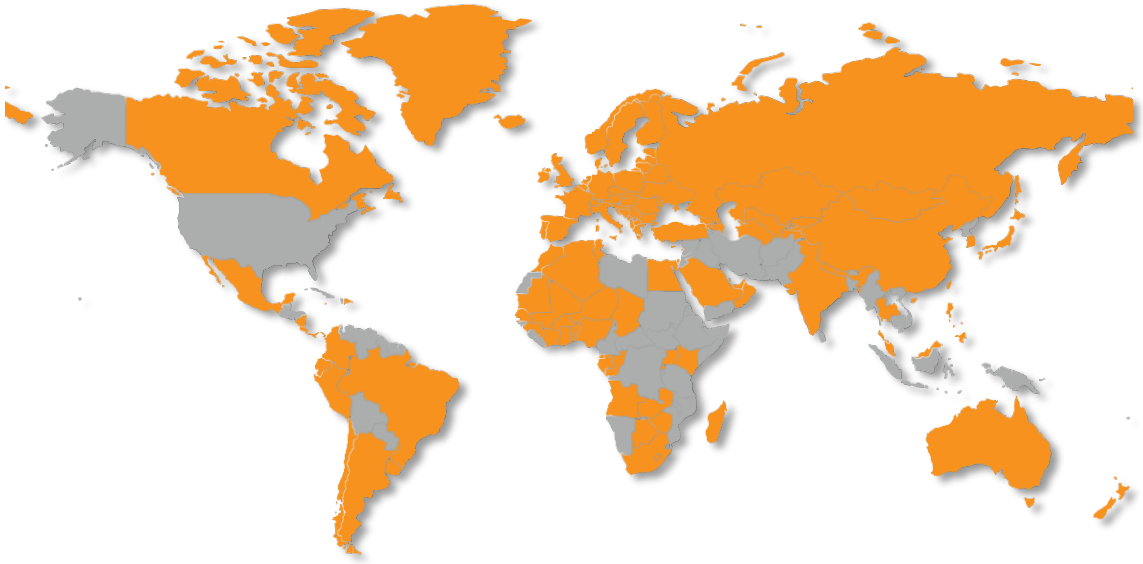
La fase final documenta el proceso de DPIA y sus conclusiones. El informe de la DPIA detalla los riesgos y las medidas paliativas. Si es necesario, la DPIA puede notificarse a una autoridad de supervisión.

Leyes

El interés por la privacidad de los datos ha aumentado en todo el mundo.

Desde la aprobación de la histórica ley GDPR en Europa, las jurisdicciones de todo el mundo han reconocido cada vez más la importancia de proteger los datos de los consumidores y han tomado medidas para exigir que las empresas manejen esa información adecuadamente.

Como se ilustra a continuación, la mayoría de los países cuentan ya con leyes de protección de datos a nivel nacional:



Ley nacional de protección de datos, 2024

GDPR

El RGPD es un reglamento de la Unión Europea (UE) que protege la privacidad y los datos personales de los ciudadanos de la UE estableciendo directrices para la recopilación, el tratamiento y el almacenamiento de información personal por parte de organizaciones y empresas.

En el momento de su aprobación, fue un logro histórico. Estableció nuevas y ambiciosas normas de protección de datos (como los requisitos de consentimiento para el tratamiento de datos, los requisitos del delegado de protección de datos y las normas de minimización de datos) y utilizó el peso geopolítico y económico de la UE para moldear para siempre los términos del debate sobre los derechos de los consumidores y la privacidad.

Sus efectos han sido globales. Con un alcance que afecta a empresas que operan totalmente fuera de la UE (lo que se conoce como "extraterritorialidad"), empresas de todo el mundo se han visto afectadas por la ley. En los años siguientes a su aprobación, el RGPD influyó considerablemente en la última de otras jurisdicciones, como la CPRA de California y la LPRPDE de Canadá.

No se puede exagerar la importancia del RGPD.

Entre los principales requisitos del RGPD figuran los siguientes

1. **Legalidad, equidad y transparencia**

Los datos personales deben tratarse de forma legal, justa y transparente en relación con el interesado. Las organizaciones deben tener una base legítima para el tratamiento de los datos, como el consentimiento, y deben informar claramente a las personas sobre cómo se utilizan sus datos.

2. **Finalidad Limitación**

Los datos recogidos deben tener fines determinados, explícitos y legítimos y no ser tratados posteriormente de forma incompatible con dichos fines.

3. **Minimización de datos**

Las organizaciones sólo deben tratar los datos personales que sean necesarios para alcanzar los fines del tratamiento. Esto significa limitar los datos recogidos a lo que sea directamente pertinente y necesario para el fin especificado.

4. **Derechos del interesado**

Las personas tienen derechos sobre sus datos, como el acceso, la rectificación, la supresión, la limitación del tratamiento, la oposición al tratamiento y el derecho a la portabilidad de los datos.

5. **Responsabilidad y protección de datos por diseño y por defecto**

Las organizaciones deben demostrar su cumplimiento aplicando los principios de protección de datos e integrando las salvaguardias necesarias en sus actividades de tratamiento de datos desde el principio (por diseño) y garantizar que, por defecto, sólo se traten los datos personales que sean necesarios para cada finalidad específica del tratamiento.

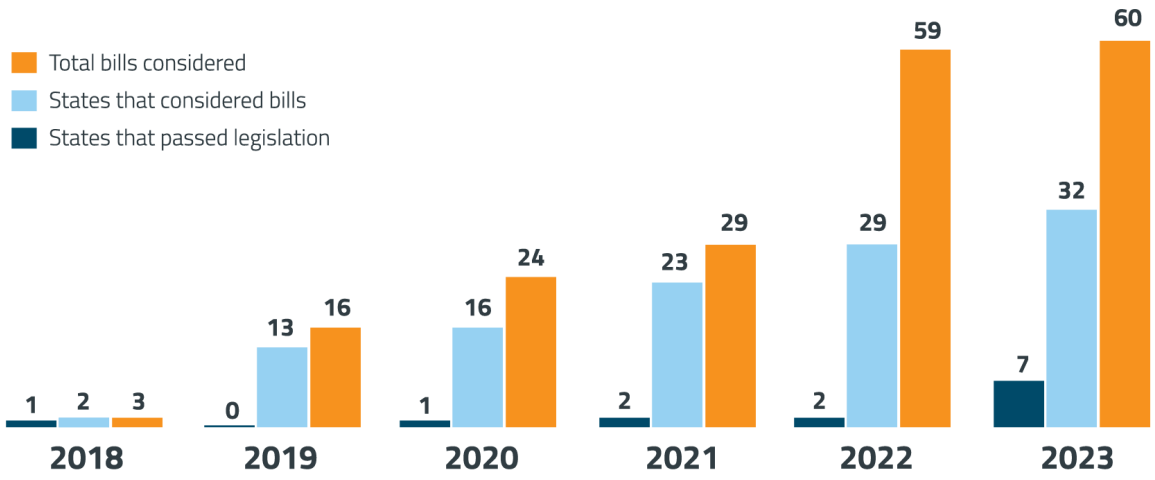
Estados Unidos

El panorama de la legislación sobre privacidad en Estados Unidos difiere significativamente del de la UE.

Estados Unidos es uno de los pocos países que carece de una legislación federal general sobre privacidad. Aunque en 2022 se presentó una nueva ley, la American Data Privacy and Protection Act (ADPPA), que obtuvo cierto respaldo en el Congreso, parece haberse estancado sin apoyo en el Senado y los analistas predicen que seguirá marginada en un futuro próximo.

Debido a la inacción federal, la legislación estadounidense sobre privacidad de datos se rige principalmente a nivel estatal.

Como hemos visto en todo el mundo, el interés por la legislación estatal sobre privacidad ha sido exponencial. El número de proyectos de ley considerados y aprobados ha aumentado notablemente en los últimos cinco años.



En muchos sentidos, 2023 fue un año decisivo para la aprobación de legislación. Se promulgaron nuevos proyectos de ley en siete estados, entre ellos los siguientes:

Delaware
Ley de Delaware sobre Protección de Datos Personales (DPDPA)

Florida
Carta Digital de Derechos de Florida (FDBR)

Indiana
Ley de Protección de Datos de los Consumidores de Indiana (ICDPA)

Montana
Ley de Protección de Datos de los Consumidores de Montana (MCDPA)

Oregón
Ley de Privacidad del Consumidor de Oregón (OCPA)

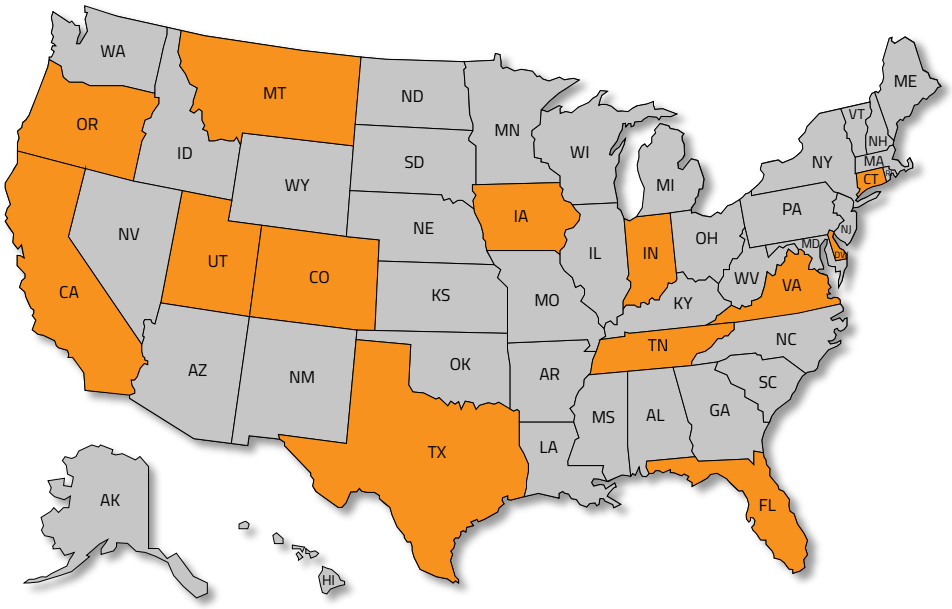
Tennessee
Ley de Protección de la Información de Tennessee (TIPA)

Texas
Ley de Privacidad y Seguridad de Datos de Texas (TDPSA)

La acción legislativa en las jurisdicciones arriba mencionadas se suma a la legislación previamente existente en los siguientes estados:

 **California** Ley de Derechos de Privacidad de California (CPRA)	 **Colorado** Ley de Privacidad de Colorado (CPA)	 **Connecticut** Ley de Privacidad de Datos de Connecticut (CDPA)
 **Iowa** Ley de Iowa (Ley relativa a la protección de datos de los consumidores)	 **Utah** Ley de Privacidad del Consumidor de Utah (UCPA)	 **Virginia** Ley de Protección de Datos de los Consumidores de Virginia (VCDPA)

Como resultado, el panorama general actual de la legislación estadounidense sobre privacidad de datos es el siguiente:



Leyes estatales de protección de datos, 2024

Aunque cada ley estatal tiene algunos puntos en común (cada una trata de aumentar los derechos de los consumidores y, por ahora, las organizaciones que quieran cumplirla tendrían que cumplir la norma aplicable más estricta entre los estados), hay suficientes diferencias que los comentaristas jurídicos se refieren a la ley de privacidad de EE.UU. como un "mosaico". Por ejemplo, los derechos de exclusión e inclusión voluntarias en la publicidad digital varían significativamente y existe la posibilidad de que se produzcan más cambios en el futuro a medida que cada estado ultime su normativa.

Por todo ello, los próximos años pueden constituir un "hito fundamental" en la convergencia de las normativas. Es de esperar que en el futuro se adopten medidas para armonizar las legislaciones estatales o se busquen formas de evitar la sobrerregulación. Aunque se trata de un objetivo a largo plazo, hay indicios de que este año podría producirse un avance significativo hacia la armonización.

Otros

Canadá

El marco actual de protección de datos en Canadá se rige principalmente por la Ley de Protección de Datos Personales y Documentos Electrónicos (PIPEDA).

Promulgada en 2000, la LPRPDE establece las normas para la recogida, uso y divulgación de información personal en el curso de actividades comerciales en todas las provincias, excepto en aquellas que tienen sus propias leyes de privacidad equivalentes. Se aplica a las organizaciones del sector privado y está supervisada por la Oficina del Comisario de Privacidad de Canadá.

La LPRPDE se basa en el principio de obtener el consentimiento para la recogida, uso y divulgación de información personal. Hace hincapié en la necesidad de que las organizaciones recojan información únicamente con fines razonables y les exige que mantengan datos exactos, completos y actualizados. Las personas tienen derecho a acceder a su información personal en poder de una organización y cuestionar su exactitud. La ley también exige medidas de seguridad adecuadas para proteger los datos personales.

A lo largo de los años, la LPRPDE ha sufrido modificaciones para responder a las nuevas preocupaciones en materia de privacidad, en particular en relación con la información digital y los flujos de datos transfronterizos. En la actualidad, se han propuesto importantes actualizaciones de las leyes nacionales de Canadá, pero aún no se han promulgado.

India

Las leyes de privacidad de datos de la India se rigen actualmente por la Ley de Protección de Datos Personales Digitales (DPDP Act), promulgada en 2023. El gobierno indio aún no ha fijado unos datos efectivos y es probable que apruebe una legislación de seguimiento que determinará cómo se aplica la ley.

The La Ley DPDP crea obligaciones para los fiduciarios de datos, entre ellas exigir el consentimiento del usuario antes del tratamiento de los datos y el establecimiento de medidas de salvaguardia para evitar infracciones. Se conceden derechos a los consumidores, entre ellos solicitar un resumen de sus datos recogidos y corregirlos, actualizarlos o eliminarlos.

La ley también crea un Consejo de Protección de Datos en India con importantes competencias para investigar posibles violaciones de la ley y hacer cumplir sus mandatos.

La Ley DPDP tiene alcance extraterritorial. Se aplica al tratamiento de datos fuera de India si está relacionado con una actividad de oferta de bienes o servicios a sujetos dentro de India. Esto significa que las empresas internacionales deben cumplir la ley al tratar datos de usuarios indios.

México

La Ley Federal de Protección de Datos Personales en Posesión de los Particulares en México es la piedra angular del marco jurídico del país en materia de protección de datos en el sector privado.

Promulgada en 2010, supuso un avance significativo en la armonización con las normas mundiales de privacidad de datos, reflejando principios como los del GDPR de la Unión Europea.

El objetivo principal de la ley es regular el tratamiento lícito, informado y leal de datos personales por parte de entidades privadas, garantizando la protección de la intimidad y los derechos fundamentales de las personas.

Obliga a los responsables del tratamiento a obtener el consentimiento explícito para el tratamiento de datos personales, salvo en las excepciones específicas previstas por la ley. Además, hace hincapié en la transparencia, obligando a los responsables del tratamiento a revelar la finalidad y los medios del tratamiento de datos.

También dota a los individuos de derechos ARCO, otorgándoles el control sobre su información personal.

Recursos

La formación continua sobre la evolución actual es vital para los profesionales, las organizaciones y las personas que manejan datos personales.

Para apoyar esta necesidad de aprendizaje continuo y cumplimiento legal, la siguiente sección presenta una lista de recursos externos.

Estos recursos, accesibles sin coste alguno, ofrecen una gran cantidad de conocimientos que van desde materiales introductorios hasta análisis en profundidad y orientaciones prácticas sobre diversos aspectos de la privacidad de los datos.

Asociación Internacional de Profesionales de la Privacidad (IAPP)

Como la mayor y más completa comunidad y recurso mundial de privacidad de la información, la IAPP ofrece una amplia formación, orientación política y recursos para los profesionales de la privacidad. Más información aquí.

Manual de Baker McKenzie sobre privacidad y seguridad de los datos a escala mundial

Este centro de recursos, creado por el bufete de abogados Baker McKenzie, ofrece orientación a las empresas para navegar por las leyes de protección de datos, privacidad y ciberseguridad en varias jurisdicciones. Más información aquí.

Cuestiones de privacidad

El Global Privacy and Data Protection Resource de DLA Piper incluye informes y análisis jurídicos de expertos sobre las tendencias en materia de privacidad de datos. Lea más aquí.

Recursos sobre la responsabilidad de los datos de Google Business

Google ofrece formación, así como acceso a herramientas analíticas gratuitas y tecnologías de privacidad de código abierto que ayudan a las empresas a comprender y gestionar sus datos de forma más eficaz y responsable. Más información aquí.

JD Supra

Este recurso incluye actualizaciones de la Ley de Privacidad, noticias y comentarios jurídicos de destacados abogados y bufetes de abogados. Lea más aquí.

Glosario

Plazo	Definición
Datos biométricos	Datos personales resultantes de tratamientos técnicos específicos relacionados con características físicas que pueden identificar a una persona.
Consentimiento	Una indicación libre, específica, informada e inequívoca de los deseos del interesado que signifique su acuerdo con el tratamiento de datos personales.
Filtración de datos	Incidente de seguridad en el que se accede a información sin autorización.
Controlador de datos	La entidad que determina los fines y medios del tratamiento de datos personales.
Minimización de datos	El principio de que los datos personales recogidos deben limitarse a lo necesario en relación con los fines para los que se tratan.

Portabilidad de datos	Derecho del interesado a recibir sus datos personales en un formato estructurado, de uso común y lectura mecánica.
Procesador de datos	Entidad que trata datos personales por cuenta del responsable del tratamiento.
Autoridad de Protección de Datos (APD)	Autoridad pública responsable de supervisar y hacer cumplir la legislación sobre protección de datos.
Sujeto de los datos	El individuo al que pertenecen los datos personales.
Datos desidentificados	Información de la que se han eliminado los identificadores para evitar una asociación directa con las personas.
Datos cifrados	Datos personales que se han transformado por medios tecnológicos para protegerlos contra el acceso no autorizado.
Reglamento general de protección de datos (RGPD)	Normativa de la UE sobre protección de datos y privacidad en la Unión Europea y el Espacio Económico Europeo.
Oficina del Comisario de Información (ICO)	Autoridad independiente del Reino Unido creada para defender los derechos de información en interés público.
Interés legítimo	Un interés razonable que el responsable del tratamiento tiene en el tratamiento de datos personales y que se contrapone a los intereses o derechos fundamentales del interesado.
Datos personales	Información relativa a una persona identificable, como nombres, números de identificación y datos de localización.
Evaluación del impacto sobre la privacidad (EIP)	Herramienta utilizada para identificar y reducir los riesgos para la privacidad de las entidades mediante el análisis del tratamiento de la información personal.
Privacidad por diseño	Principio que exige tener en cuenta la privacidad a lo largo de todo el proceso de ingeniería de un producto o servicio.

Tratamiento	Cualquier operación realizada con datos personales, desde su recogida hasta su destrucción.
Perfil	Cualquier forma de tratamiento automatizado de datos personales para evaluar determinados aspectos personales relativos a una persona física.
Pseudonimización	Tratar los datos personales de tal forma que ya no puedan atribuirse a un interesado concreto sin utilizar información adicional.
Derecho al olvido	Derecho de las personas a que se supriman sus datos personales en determinadas circunstancias.
Datos personales sensibles	Datos personales que incluyan datos genéticos, biométricos, relativos a la salud, al origen racial o étnico, a las opiniones políticas o a la orientación sexual.
Solicitud de acceso del interesado (SAR)	Solicitud de un interesado para obtener una copia de los datos personales que una organización tiene sobre él.
Terceros	Cualquier entidad que no sea el interesado, el responsable del tratamiento, el encargado del tratamiento o las personas autorizadas a tratar datos personales bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento.
Transparencia	El principio de que la información sobre el tratamiento de datos personales debe ser fácilmente accesible y comprensible para el interesado.
Autenticación de dos factores (2FA)	Proceso de seguridad en el que el usuario proporciona dos factores de autenticación diferentes para verificarse.
Datos no estructurados	Información que no reside en una base de datos tradicional de filas y columnas y que suele contener mucho texto.
Datos del usuario	Datos relacionados con el comportamiento y la interacción de los usuarios con servicios o productos, a menudo recopilados a través de actividades en línea.

Infracción	Incumplimiento de la legislación sobre protección de datos, que puede dar lugar a acciones coercitivas y sanciones.

Acerca de VENZA

VENZA es el proveedor líder de protección de datos y cumplimiento normativo para el sector hotelero. Basándose en décadas de experiencia, VENZA proporciona una visibilidad de 360 grados que permite una gestión proactiva de los riesgos para mitigar las vulnerabilidades y mantener a salvo a sus huéspedes y sus datos. Conozca sus riesgos y proteja su empresa con VENZA..

Visite www.VENZAGroup.com para obtener más información.

Póngase en contacto con nosotros

Ventas: sales@venzagroup.com

Éxito de clientes: success@venzagroup.com