ABC

GUÍA ESTRATÉGICA DE CUMPLIMIENTO DE PRIVACIDAD DE ESTADOS UNIDOS

OLARTEMOURE
OLARTE MOURE & ASOCIADOS
Abogados - Attorneys

Escríbenos: info@olartemoure.com

Introducción

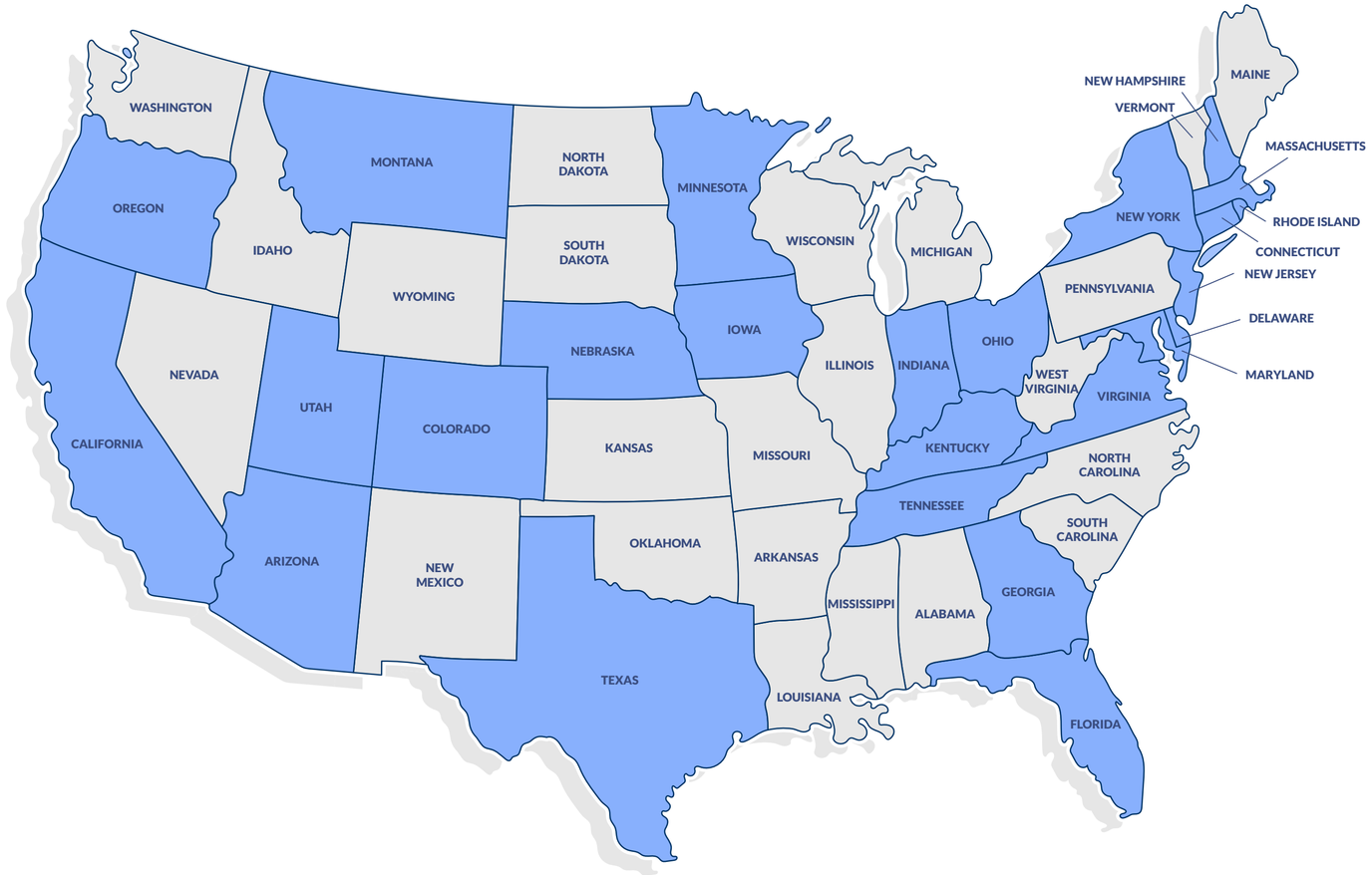
La regulación de la protección de datos personales en Estados Unidos se caracteriza por un enfoque sectorial, pues no hay una ley federal general, que abarque la totalidad de escenarios de tratamiento de datos personales, como sí sucede con el Reglamento General de Protección de Datos la Unión Europea, la Ley 1581 de 2012 de Colombia y otras regulaciones nacionales en diversas jurisdicciones. A nivel federal, solo rigen leyes específicas por sector o tipo de datos (por ejemplo, la ley de protección de datos de salud -HIPAA-, la ley de protección de información financiera -GLBA-, la ley de protección de la privacidad infantil en línea -COPPA-, la ley de informes crediticios -FCRA-, entre otras).

Desde 2018, varios estados han promulgado sus propias leyes generales de privacidad. Concretamente, California, como estado pionero en esta materia, promulgó el California Consumer Privacy Act (“CCPA”) y el California Privacy Rights Act (“CPRA”), y en los años siguientes muchos estados le han seguido. Actualmente, alrededor de 25 estados cuentan con leyes estatales de protección de datos con un alcance más amplio, que se encuentran vigentes o entrarán en vigor durante 2026. No obstante, es importante mencionar que un número importante de estas regulaciones están enfocadas en la privacidad de los consumidores.

Además de las leyes estatales, algunos estados han adoptado regulaciones específicas aplicables a determinados sectores o tipos de tratamiento de datos. Illinois, por ejemplo, cuenta desde 2008 con la Biometric Information Privacy Act (BIPA), considerada una de las normas más estrictas en materia de protección de datos biométricos. Otros estados, como Nevada y Delaware, han expedido disposiciones que obligan a ofrecer a los titulares la posibilidad de optar por excluirse (opt-out) de la venta de sus datos personales. Este modelo parte de la premisa de que los datos pueden ser comercializados por defecto, salvo que el titular manifieste lo contrario, y se encuentra en contraposición con el sistema opt-in, en el cual la venta o cesión de datos únicamente procede cuando el titular otorga su consentimiento previo, libre e informado.

A diferencia de Estados Unidos, la mayoría de los países han adoptado leyes generales de protección de datos personales. Actualmente, más de 160 jurisdicciones en el mundo cuentan con este tipo de normativa, incluidas prácticamente todas las economías desarrolladas. En la Unión Europea rige desde 2018 el Reglamento General de Protección de Datos (GDPR), considerado el estándar internacional en la materia. En América Latina, casi todos los países han expedido leyes nacionales en la última década, como Colombia, México, Brasil, Argentina, Chile, Ecuador y Uruguay.

Protección de datos en EE.UU



Cuentan con leyes de protección de datos personales o regulaciones similares.

No cuentan con leyes de protección de datos personales o regulaciones similares.

Arizona	Ley de Notificaciones de Brechas de Seguridad	Ohio	Normativa de Protección de Datos de Ohio
California	Ley de Privacidad del Consumidor (CCPA/CPRA)	Oregon	Ley de Privacidad del Consumidor de Oregon
Virginia	Ley de Protección de Datos de Virginia (VCDPA)	Delaware	Ley de Privacidad de Datos Personales de Delaware
Colorado	Ley de Privacidad de Colorado (CPA)	New Hampshire	Ley de Privacidad de New Hampshire
Connecticut	Ley de Privacidad de Datos de Connecticut	New York	Ley de Privacidad y Seguridad de Datos
Utah	Ley de Privacidad del Consumidor de Utah (UCPA)	New Jersey	(Ley de Privacidad de NJ, aprobada en 2022/23)
Iowa	Ley de Privacidad de Datos de Iowa	Kentucky	(Ley de Privacidad de Kentucky, aprobada en 2024)
Indiana	Ley de Privacidad del Consumidor de Indiana	Nebraska	(Ley de Privacidad de Nebraska, aprobada en 2023)
Tennessee	Ley de Privacidad de Tennessee	Rhode Island	Ley de Transparencia y Privacidad de Datos de Rhode Island
Texas	Ley de Privacidad de Datos de Texas (TDPSA)	Massachusetts	Ley de Privacidad de la Información de Massachusetts
Florida	Ley de Derechos de los Datos Digitales de Florida (FDBR)	Maryland	Ley de Privacidad en Línea de Maryland (MODPA)
Georgia	Ley de Protección de Identidad de Georgia	Minnesota	Ley de Privacidad de Datos de Minnesota
Montana	Ley de Privacidad de Datos del Consumidor de Montana		

(Nota: Varias de estas leyes han entrado en vigor recientemente o lo harán entre 2025 y 2026, por lo que su aplicación práctica está en desarrollo)

En términos generales, estas normas se aplican a las empresas que tratan datos personales de residentes del estado, siempre que superen ciertos umbrales de volumen de datos o ingresos, y suelen excluir a las pequeñas empresas. Cabe resaltar que ello implica un cierto grado de extraterritorialidad, en la medida en que la obligación de cumplimiento no depende de que la empresa esté físicamente establecida en el estado, sino de que trate datos de sus residentes. Dichas leyes otorgan a los individuos derechos como acceder, corregir, eliminar, obtener copias, optar por no participar en la venta o en la publicidad dirigida, y restringir el uso de datos sensibles.

Al mismo tiempo, imponen a las empresas obligaciones de transparencia, seguridad y responsabilidad, entre ellas: proporcionar avisos de privacidad claros, establecer límites al uso de datos, proteger información sensible, suscribir contratos con proveedores, realizar evaluaciones de riesgo en determinados casos y atender oportunamente las solicitudes de los titulares.

En los estados sin una ley general de privacidad, aplica el marco mínimo federal y disposiciones estatales específicas, como las leyes de notificación de brechas de seguridad, normas sobre información de salud o educación, restricciones al uso del número de Seguridad Social y reglas de eliminación segura de documentos.

Obligaciones del responsable de datos

¿CUÁLES SON LAS OBLIGACIONES DE UN RESPONSABLE DEL TRATAMIENTO DE DATOS PERSONALES EN ESTADOS UNIDOS?

En el entorno normativo estadounidense, un Responsable del tratamiento debe implementar una serie de políticas y procedimientos internos para asegurar el cumplimiento de las diversas leyes aplicables. De manera particular, las principales actividades y medidas que un Responsable debe llevar a cabo para alinearse con las regulaciones de datos personales en Estados Unidos son:

1. POLÍTICA DE PRIVACIDAD:

Un primer requisito esencial para cualquier Responsable en Estados Unidos es contar con una Política de Privacidad pública, clara y actualizada. Este documento debe explicar de manera general cómo la empresa recolecta, utiliza, comparte y protege los datos personales. Su función principal es otorgar transparencia frente a consumidores y autoridades, y se convierte en la base del programa de cumplimiento en materia de protección de datos.

2. AVISOS DE PRIVACIDAD (PRIVACY NOTICES):

Además de la política general, muchas leyes exigen avisos específicos en el punto de recolección de datos. Por ejemplo, la CCPA/CPRA en California obliga a informar al consumidor antes de capturar su información, detallando las categorías de datos que se recopilarán y la finalidad del tratamiento. En el caso de datos biométricos, la BIPA de Illinois requiere un consentimiento expreso y por escrito, así como un aviso que informe sobre la finalidad y la duración de la retención.

Cuando se trata de menores de edad, deben cumplirse reglas adicionales: la COPPA (federal) exige consentimiento parental para menores de 13 años, mientras que California prohíbe la venta de datos de menores de 16 sin un consentimiento expreso. Esto implica que las empresas deben diseñar flujos de autorización, con casillas de aceptación o formularios electrónicos, y mantener registros de esos consentimientos.

3. MEDIDAS DE SEGURIDAD DE LA INFORMACIÓN:

La normativa estadounidense exige la implementación de medidas de seguridad razonables, proporcionales al tipo de datos tratados y a la magnitud de la empresa. Aunque no existe un estándar único obligatorio, se espera que el Responsable desarrolle una política interna de seguridad de la información acompañada de controles técnicos y organizativos que garanticen la confidencialidad, integridad y disponibilidad de los datos. Este punto constituye uno de los pilares fundamentales de la protección de la información personal.

4. GESTIÓN DE INCIDENTES Y BRECHAS DE SEGURIDAD:

Otro componente clave es la gestión de incidentes de seguridad. En Estados Unidos, todos los estados cuentan con leyes que exigen notificar a los afectados cuando ocurre una brecha que compromete sus datos personales. En algunos casos, también se debe informar a las autoridades, como sucede en California o Massachusetts.

Por lo tanto, el Responsable debe implementar un Plan de Respuesta a Incidentes que contemple procedimientos para identificar, contener, investigar y remediar una filtración de datos. Además, la normativa fija plazos estrictos para las notificaciones (entre 30 y 60 días, dependiendo del estado). La preparación previa, incluyendo simulacros de brechas y seguros de ciberriesgo, resulta indispensable para gestionar eficazmente estos escenarios.

Obligaciones del responsable de datos

5. CONTRATOS CON ENCARGADOS (SUPPLIERS/PROCESSORS):

Cuando la empresa comparte datos con terceros que actúan en su nombre, debe hacerlo bajo un contrato formal de protección de datos. Dichos contratos deben limitar el uso de la información exclusivamente a las instrucciones del Responsable, exigir medidas de seguridad y confidencialidad, prever la devolución o eliminación de los datos al finalizar la relación, y establecer la obligación de colaborar en auditorías o notificaciones de incidentes. Un ejemplo claro es la CCPA en California, que solo permite considerar como “prestación de servicios” –y no como “venta de datos”– aquellas transferencias que están cubiertas por un contrato con estas cláusulas mínimas. De igual manera, otras leyes estatales (Virginia, Colorado, Connecticut, entre otras) incluyen requisitos similares.

6. EVALUACIONES DE IMPACTO EN PRIVACIDAD (PIA/DPIA):

Un ámbito emergente en el cumplimiento estadounidense es la realización de evaluaciones de impacto en privacidad. Estas evaluaciones deben llevarse a cabo cuando la organización despliega nuevas tecnologías o iniciativas que puedan afectar los derechos de los titulares. El ejercicio consiste en documentar las finalidades del tratamiento, los beneficios y los riesgos que genera, así como las medidas de mitigación implementadas. Su principal valor es demostrar que la empresa aplica principios de privacidad desde el diseño y que analiza preventivamente los efectos sobre las personas.

7. POLÍTICAS DE IA:

Finalmente, la creciente regulación en Estados Unidos está enfocando su atención en la inteligencia artificial y las tecnologías de decisión automatizada (ADMT). Legislaciones recientes en California imponen a las empresas que utilicen estas tecnologías obligaciones de transparencia reforzada. En particular, los Responsables del tratamiento deben desarrollar Políticas de Inteligencia Artificial que informe sobre el uso de la misma al interior de la Organización.

¿Es necesario contar con un DPO en Estados Unidos?

A diferencia del Reglamento General de Protección de Datos (GDPR) en Europa, que sí exige la designación de un Delegado de Protección de Datos (Data Protection Officer – DPO) en determinados supuestos, en Estados Unidos no existe una figura única ni estandarizada equivalente al DPO. Las leyes de privacidad estatales no utilizan ese término ni imponen de manera general la obligación de crear dicho cargo.

Sin embargo, varias de estas normas sí exigen designar a una persona responsable del cumplimiento de la regulación en materia de datos personales. En algunos casos, la exigencia se traduce en la obligación de nombrar formalmente a un encargado interno con funciones específicas de privacidad. Por ejemplo, la nueva ley de privacidad de Minnesota requiere que las organizaciones designen un Chief Privacy Officer (“CPO”) como responsable de supervisar la aplicación de la normativa.

En conclusión, aunque en Estados Unidos no existe la figura uniforme de un DPO como en Europa, sí se observa una tendencia regulatoria a exigir que las empresas designen un responsable interno de privacidad. Por ello, resulta recomendable que las organizaciones nombren a un oficial, sea CPO, DPO o cargo similar, para coordinar el cumplimiento normativo, responder a autoridades y preparar a la empresa frente a nuevas obligaciones legales.

OLARTEMOURE

OLARTE MOURE & ASOCIADOS

Abogados - Attorneys

Contáctenos para mayor información

info@olartemoure.com