



# Legislación sobre la protección de datos

**recall**<sup>TM</sup>  
Your Information. Securely Managed.

## Legislación sobre la protección de datos

La posibilidad de rastrear, seguir y encontrar datos importantes es esencial cuando se deben cumplir requisitos normativos como:

### Ley de Gramm-Leach-Bliley (GLBA), 1999

La ley GLBA requiere que las instituciones financieras aporten herramientas administrativas, técnicas y físicas para proteger la integridad y la confidencialidad de los registros de sus clientes. Las empresas también deben garantizar la disponibilidad de la información financiera y la continuidad comercial. El no cumplimiento pueden suponer multas de hasta 1 millón de dólares además de otras penas.

### Ley Sarbanes-Oxley (SOX), 2002

La ley SOX surge como respuesta directa a los escándalos de empresas como Enron and WorldCom. Su normativa garantiza la integridad de la información financiera y aborda la gestión corporativa. La ley SOX afecta a las compañías públicas de EE.UU pero su impacto puede ser mundial para sus empleados, juntas y auditores, ya que puede hacerles responsables a título personal de la corrección y del mantenimiento de la información financiera. Se pueden aplicar sanciones y multas significativas, que incluyen, además, periodos de encarcelamiento.

### Ley de responsabilidad y transferibilidad de los seguros médicos (HIPAA), 1996

La ley HIPAA fue aprobada para proteger la cobertura de seguro médico a los trabajadores y sus familias cuando éstos cambian o pierden sus empleos. Artículo uno, Título II, se requiere de la creación de estándares para los registros electrónicos sanitarios de pacientes, datos administrativos y financieros y la protección seguridad de datos relacionados a la salud. HIPAA puede afectar a toda organización involucrada o relacionada con la salud. Se puede extender a empresas que ofrecen servicios al área de salud, como por ejemplo los proveedores del sistema de información. Aunque la HIPAA no indica medidas de cumplimiento, el no proteger de manera razonable la información cubierta por dicha ley puede implicar la aplicación de una multa de hasta 250.000 USD y penas hasta 10 años de prisión.

Se solicitan auditorías programadas o en curso para la confirmación de la exactitud y disponibilidad de la información específica de los actos arriba mencionados. Con frecuencia, los sistemas se prueban para garantizar la entrega oportuna de información relevante. Además, el periodo de retención puede ser de hasta 7 años para los datos financieros y para el sector sanitario, mientras que los datos manejados por éste es posible que tengan que guardarse durante más de 20 años. La clave está en que esta información debe estar disponible en cualquier momento y que su contenido puede abarcar un periodo de tiempo considerable.

En Australia, la Ley de privacidad de 2001, Artículo 4, Almacenaje y seguridad de información personal, requiere que el “que guarda” los registros garantice que la información contenida en los mismos esté protegida frente a pérdidas, acceso y utilización no autorizados, modificación, publicación y otras formas de uso indebido, para lo que deberá llevar a cabo medidas de seguridad razonables y en la medida de sus posibilidades. El incumplimiento responsabilizará personalmente al guardián de los registros y sujeto a juicio.

Aproximadamente en todos los países donde Recall realiza operaciones, introdujo alguna forma de legislación para garantizar la protección de la información sensible. En general, se basa en finanzas y fue iniciada por la autoridad del servicio financiero o monetario del país. Para la Unión Europea, véase la Directiva relativa los mercados de instrumentos financieros (MiFID) y para el Reino Unido, las Leyes de protección de datos y de libertad de información.

\* Fuente: B&L Associates, “Compliance through Proper Tape Management”