CrashPlan + GLBA

CrashPlan

TECH OVERVIEW

CrashPlan supports customer compliance with GLBA requirements, giving organizations the critical data backup and recovery capabilities needed to protect their customers' private information. CrashPlan provides a powerful data protection foundation that contributes to a long-term GLBA compliance strategy and prepares organizations to meet evolving regulations and complex compliance requirements.

What is GLBA?

The Gramm-Leach-Bliley Act (GLBA) is also known as the Financial Modernization Act of 1999. It is a United States federal law that requires financial institutions to explain how they share and protect their customers' private information. GLBA applies to all businesses, regardless of size, that are "significantly engaged" in providing financial products or services. This includes, for example, mortgage brokers, payday lenders, non-bank lenders, real estate appraisers, and professional tax preparers.

The GLBA requires financial institutions ensure the confidentiality and security of customers' nonpublic personal information (NPI), which includes Social Security numbers, credit and income histories, credit and bank card account numbers, phone numbers, addresses, names, and any other personal customer information received by a financial institution that is not public.

What Are the Possible Penalties for Non-Compliance?

- **Financial institutions found in violation face fines of $100,000 for each violation**
- **Individuals in charge found in violation face fines of $10,000 for each violation**
- **Individuals found in violation can be put in prison for up to 5 years**

What Are Some of the Key Requirements?

GLBA EXPANDS CUSTOMER RIGHTS FOR FINANCIAL INSTITUTIONS, INCLUDING:

- **Customers' NPI must be secured against unauthorized access**
- **Customers must have the ability to opt out of NPI sharing with other 3rd parties**
- **User activity must be tracked, including any attempts to access NPI**
- **Entities must create a written information security plan describing the program to protect their customers' NPI**

GLBA UTILIZES THE "SAFEGUARDS RULE" TO OUTLINE PRIMARY DATA PROTECTION REQUIREMENTS FOR ORGANIZATIONS, INCLUDING:

- **Designate one or more employees to coordinate its information security program**
- **Design and implement a safeguards program and regularly monitor and test it**
- **Select service providers that maintain appropriate safeguards. Make sure your contract requires them to maintain safeguards and oversee their handling of NPI**

- **Identify and assess the risks to NPI in each relevant area of the company's operation and evaluate the effectiveness of the current safeguards for controlling these risks**
- **Institutions must pay special attention to employee management and training, information systems, and security management**

How Does CrashPlan Enable Our Customers to Comply With GLBA?

CrashPlan enables customers to comply with GLBA and protect customer NPI. CrashPlan is configured by default to encrypt user data files at the source using AES 256-bit encryption, utilizing FIPS 140-2 validated modules — so you can safely backup and recover your files while mitigating risk and noncompliance and avoid associated penalties and other impacts, including reputational damage.

All data transferred to CrashPlan is encrypted at rest and in transit. Data is not used for any purpose other than as agreed upon for the provision of our products and services.

CrashPlan's Master Services Agreement incorporates an Information Security Addendum (ISA), which includes CrashPlan's commitments to safeguard your data.

Read the ISA

CrashPlan

Corporate Headquarters
400 S 4th St Suite 410
PMB 31083
Minneapolis, MN 55415-1419
612.464.2112

crashplan.com

CrashPlan® provides peace of mind through secure, scalable, and straightforward endpoint data backup. We help organizations recover from any worst-case scenario, whether it is a disaster, simple human error, a stolen laptop, ransomware or an as-of-yet undiscovered calamity. We continue to innovate as the landscape of work evolves, which makes CrashPlan foundational to organizations' data security. What starts as endpoint backup and recovery becomes a solution for ransomware recovery, breaches, migrations, and legal holds.

For more information, visit **crashplan.com**.