Gramm-Leach-Bliley Act (GLBA) Data Sanitization Requirements

“The Gramm-Leach-Bliley Act requires financial institutions - companies that offer consumers financial products or services like loans, financial or investment advice, or insurance - to explain their information-sharing practices to their customers and to safeguard sensitive data.”

Who must comply?

“The definition of “financial institution” includes many businesses that may not normally describe themselves that way. In fact, the Rule applies to all businesses, regardless of size, that are “significantly engaged” in providing financial products or services. This includes, for example, check-cashing businesses, payday lenders, mortgage brokers, nonbank lenders, personal property or real estate appraisers, professional tax preparers, and courier services. The Safeguards Rule also applies to companies like credit card reporting agencies and ATM operators that receive information about the customers of other financial institutions. In addition to developing their own safeguards, companies covered by the Rule are responsible for taking steps to ensure that their affiliates and service providers safeguard customer information in their care.”

GLBA and Information Disposal

“Dispose of customer information in a secure way and, where applicable, consistent with the FTC’s Disposal Rule. For example:

- Consider designating or hiring a records retention manager to supervise the disposal of records containing customer information. If you hire an outside disposal company, conduct dues diligence beforehand by checking references or requiring that the company be certified by a recognized industry group.
- Burn, pulverize, or shred papers when disposing of computers, disks, CDs, magnetic tapes, hard drives, PDAs, cell phones, or any other electronic media or hardware containing customer information.”

What is Data Sanitization?

According to the International Data Sanitization Consortium, “Data Sanitization is the process of deliberately, permanently and irreversibly removing or destroying the data stored on a memory device to make it unrecoverable. A device that has been sanitized has no usable residual data, and even with the assistance of advanced forensic tools, the data will not ever be recovered. There are three methods to achieve data sanitization: physical destruction, cryptographic erasure, and data erasure.”

Although data destruction and data sanitization have similarities in their approach, they are not the same. Data destruction does not include verification or certification of successful destruction beyond forensic recovery. This means that the chosen data destruction method has not been proven to remove data in totality, whether that target data is a single file or an entire drive.

Visit www.clarabyte.com to read our eBook on Data Sanitization Best Practices.

GRAMM-LEACH-BLILEY ACT (GLBA)

SPECIFICATION	DATA SANITIZATION SIMPLIFICATION
Article 682.3 -- Proper disposal of consumer information - states that “Any person who maintains or otherwise possesses consumer information for a business purpose must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal. “In this instance, “disposal” refers to the “discarding or abandonment of consumer information” or “The sale, donation, or transfer of any medium, including computer equipment, upon which consumer information is stored.” The article also states that “Reasonable measures to protect against unauthorized access to or use of consumer information in connection with its disposal include… implementing and monitoring compliance with policies and procedures that require the destruction or erasure of electronic media containing consumer information so that the information cannot practicably be read or reconstructed.”	“Reasonable measures” should be interpreted as implementing a data sanitization policy. Prove compliance with tamper-proof data sanitization reports.

Protect Consumer information with Clarabyte’s Data Sanitization Solutions

Clarabyte’s intuitive and flexible data erasure software allows highly regulated organizations to easily automate their data sanitization processes to improve security, eliminate the risk of human error when processing devices, and to guarantee compliance with GLBA. Clarabyte’s proprietary algorithm offers data erasure for the entire spectrum of hard drives and solid-state drives, with verification of successful erasure, and tamper-proof reporting. This unmatched level of control over data removal provides assurance that no trace of target data remains on a device and compliance is guaranteed.

Click here to learn more about ClaraWipe Pro.

References:

https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act

https://www.ecfr.gov/cgi-bin/text-idx?SID=a8939d3559b7c35cea1bd0065bf9496c&mc=true&node=se16.1.682_13&rgn=div8

https://www.datasanitization.org/