



THE IMPORTANCE OF DATA ERASURE

An insights report from Certus





THE IMPORTANCE OF DATA ERASURE

More data is being created and stored than ever before. As companies collect more information, and as individuals value their data privacy more, it becomes increasingly important to manage and dispose of data securely, especially when that data is no longer needed, or when a device containing confidential data changes hands.

This report will examine the importance of data erasure, explore some of the global compliance standards that provide a framework for excellence, and set out the steps to ensure data across your organization is erased safely and permanently – and that the erasure is subsequently verified.

If you have any questions about data erasure or any of the points raised in this report, you can contact our team using the details on page 9.

A handwritten signature in black ink, reading "Ruud de Wildt".

Ruud de Wildt
CEO of Certus Software GmbH

Data erasure refers to the process of securely and permanently deleting data from a storage device, ensuring it cannot be recovered or reconstructed. This is achieved through recognized techniques such as overwriting and firmware-based methods, which ensure that sensitive data is fully and permanently removed.

THERE ARE TWO PRIMARY TECHNIQUES USED FOR DATA ERASURE:

1

Overwrite

This method involves replacing the existing data on the storage device with random or predefined patterns multiple times, making the original data irretrievable.

2

Firmware-based techniques

Firmware-based techniques: These techniques use the device's firmware to execute erasure processes that affect both the user data and critical areas such as the service area and firmware, ensuring complete data removal.

Both methods follow recognized data sanitization standards, ensuring sensitive information is fully protected from unauthorized access.



MEETING PRIVACY REQUIREMENTS

Data can be stored by organizations on any number of devices including a desktop, laptop, tablet, smart phone, USB stick, server or external hard drive. Whenever that device changes ownership – whether that’s because it’s been reused (including elsewhere within the same organization), sold or decommissioned – or if individuals exercise their right under privacy laws to have personal data deleted, then certified data erasure is required.

Simply deleting files from a file manager, resetting a smartphone to factory settings or formatting a storage drive from the operating system is not enough, because that data can still be recovered. Device manufacturers often avoid taking responsibility, to make sure there’s no liability if the data erasure process fails.

Instead, certified erasure offers an enhanced level of certainty and protection, ensuring that all data is completely erased and cannot be recovered. It’s no longer a ‘nice to do’ – it’s a necessity, in an era where data privacy is vital.

WHO STORES DATA?



Enterprises



Governments



Cloud service providers



Data centers



Healthcare organizations



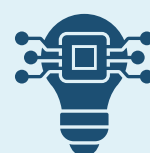
Financial institutions



Educational institutions



Telecommunications providers



Technology companies

THREE STEPS TO CERTIFIED DATA ERASURE:

1



Identify what data you have, where it is stored, and what needs to be erased.

2

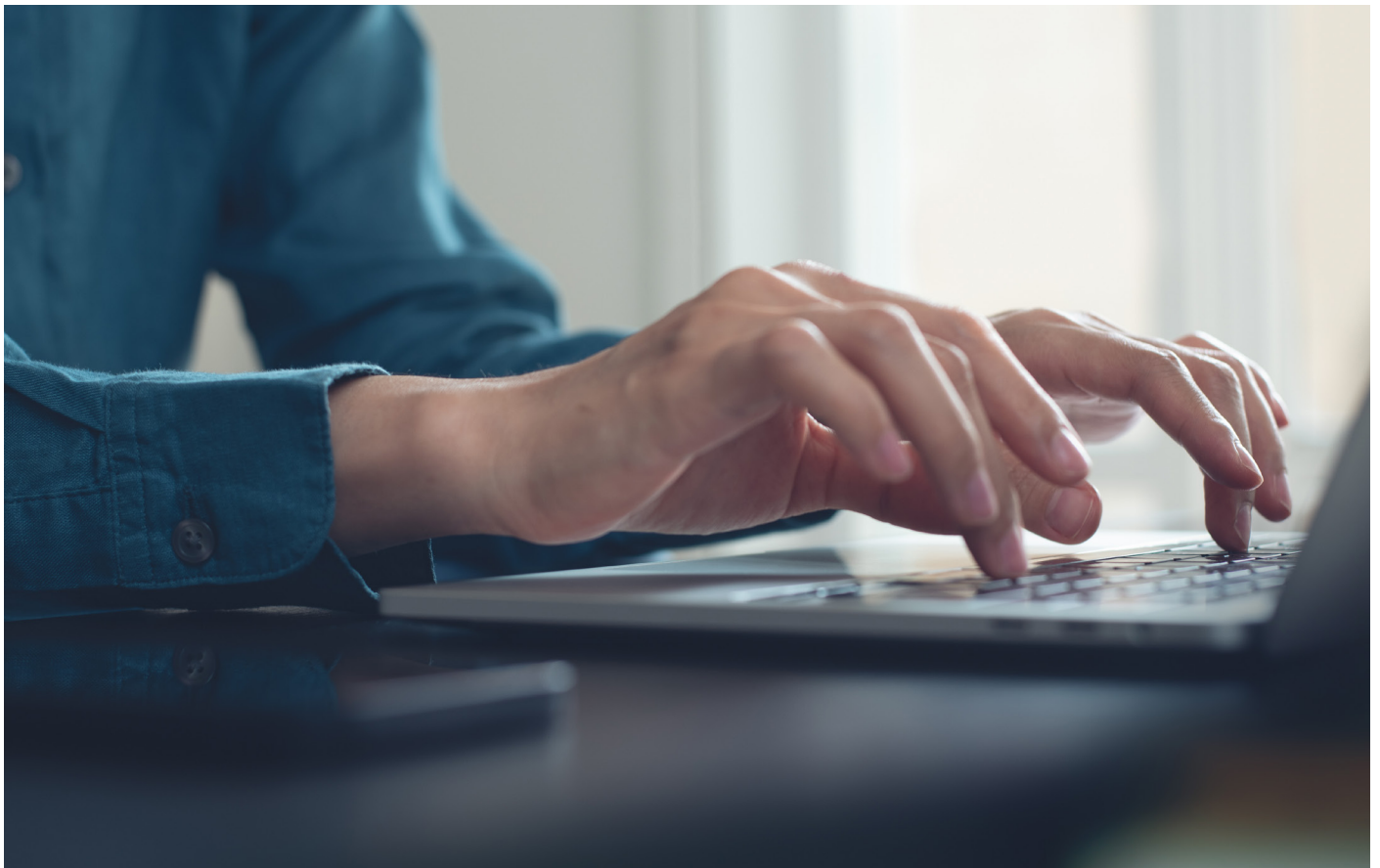


Choose a certified solution that meets your needs and complies with the necessary industry standards.

3



Following erasure, receive a Certified Data Erasure Report.



WHY IS DATA ERASURE IMPORTANT?

There are two main reasons why it is becoming increasingly important to manage your responsibilities when it comes to data erasure.

Firstly, businesses hold vast amounts of data, including confidential data – more than ever before.

- Estimates suggest that 90% of the world's data was generated in the last two years alone.¹
- 79% of global companies collect personal data on individuals living in North America, Western Europe.²
- 94% of small businesses, 97% of medium businesses and 100% of large businesses in the UK keep digital data on their employees. In addition, 93% of large businesses use digitized personal data for individuals that aren't employees.³
- 75% of consumers said they will not purchase from organizations they don't trust with their personal data.⁴

In addition, data confidentiality is more valued and more understood than ever before. If any old data isn't securely erased, it could fall into the wrong hands. This can lead to data breaches, which puts the organization at risk of financial penalties and significant reputational damage.

In the EU, GDPR requires companies to securely erase confidential data when it's no longer needed, and can impose fines of up to €20 million or 4% of a company's annual global turnover for non-compliance – that's a huge potential penalty.

- 73% of consumers are more concerned about their data privacy now than they were a few years ago.⁵
- 87% of consumers say they would not do business with a company if they had concerns about its security practices.⁶
- In 2024, GDPR fines across Europe totaled €1.2 billion. The record year for GDPR fines was 2023, when fines totaled €2.9 billion.⁷

Sources:

1. [Exploding Topics](#)
2. [Statista](#)

3. [UK Government](#)
4. [Cisco](#)

5. [SAS](#)
6. [McKinsey](#)

7. [DLA Piper](#)

SECURE DATA ERASURE AND VERIFICATION

Data erasure is considered secure when it follows recognized standards, is verifiable, and ensures data is permanently unrecoverable.

FOLLOWING RECOGNIZED STANDARDS

There are a specific set of requirements that a data erasure software platform must meet to classify as 'certified'.

Firstly, it must be tested and evaluated by experts that will simulate various attack methods, to make sure data can't be recovered. It must gain formal approval from a certification body, which will evaluate the software against stringent criteria. And finally, it must also comply with established standards and legislative frameworks designed to protect individuals' data.

These certifications, standards and legislations include:

- **ISO/IEC 15408:** Also known as the Common Criteria for Information Technology Security Evaluation, this is an international standard for assessing the security of IT products and systems. It provides a structured framework for evaluating security functions and assurance levels, allowing users, developers, and evaluators to define security requirements and verify compliance.
- **NIST SP 800-88 Rev. 1:** This guidance document provides recommendations for securely erasing data from storage devices to prevent unauthorized access to sensitive information. It defines methods such as clearing, purging and destroying data based on the level of security required, to support effective erasure of electronic media while ensuring compliance with data protection and privacy regulations.
- **IEEE 2883:2022:** Also defines guidelines for securely erasing data from storage devices to prevent unauthorized recovery. It provides methods for data sanitization, including clear, purge and destroy, applicable to various storage technologies such as hard drives, solid-state drives, and removable media. This standard aligns with industry best practices and regulatory requirements, providing a framework for compliance and best practice.
- **The General Data Protection Regulation (GDPR):** EU privacy law to protect individuals' personal data, GDPR establishes strict rules for how organizations collect, process, store and share personal information. GDPR grants individuals greater control over their data, including rights to access, correct and delete their information. It also imposes significant penalties for non-compliance.

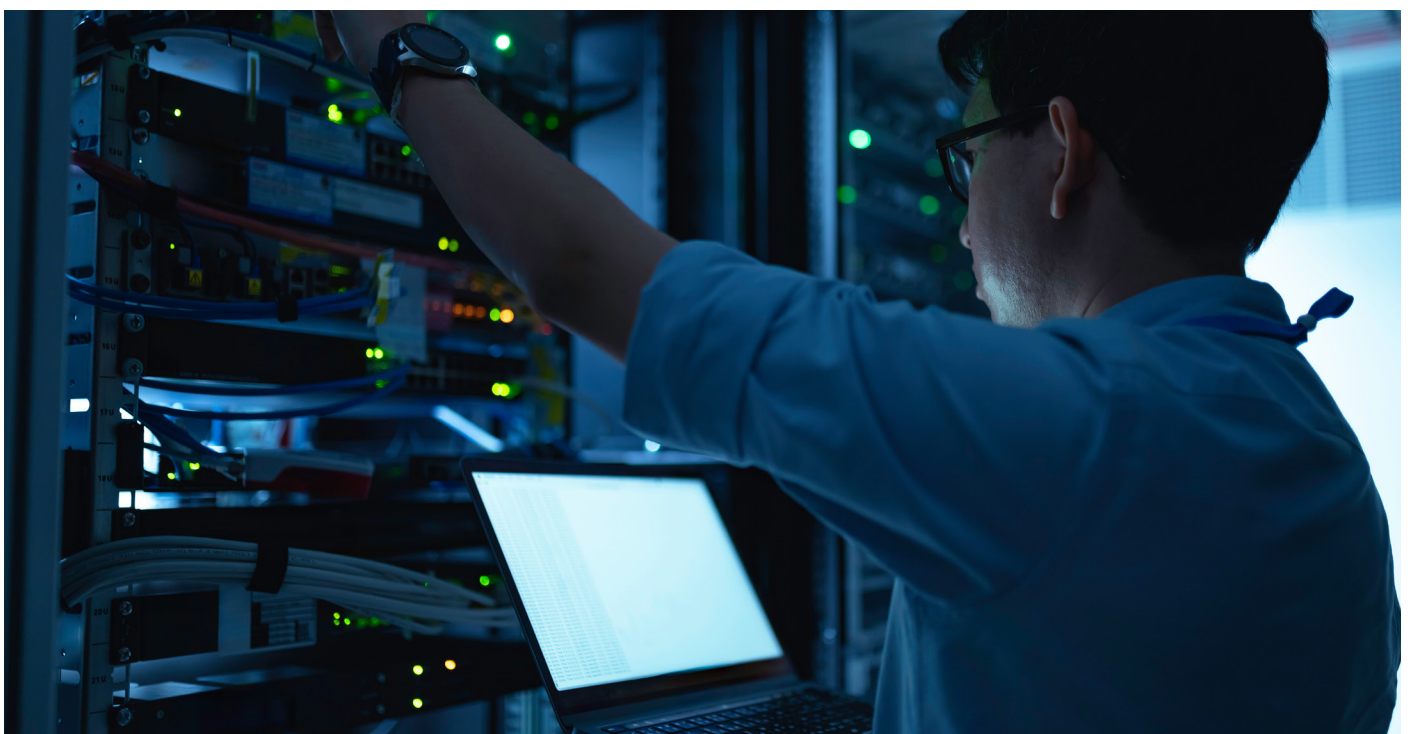
- **The Health Insurance Portability and Accountability Act (HIPAA):** A U.S. federal law which establishes rules for the privacy, security and confidentiality of medical records and personal health data, applying to healthcare providers, insurers, and related entities. HIPAA includes the Privacy Rule, which governs the use and disclosure of health information, and the Security Rule, which sets standards for protecting electronic health data.

Certified data erasure should also come with verification, assuring that the process followed meets specific compliance requirements. For compliance with NIST SP 800-88 Rev. 1 and IEEE 2883:2022, for example, it is essential that drives erased with specific software undergo verification using a different software solution. This practice ensures compliance with data removal standards and enhances the reliability of the process.

ENSURING DATA IS PERMANENTLY UNRECOVERABLE

Another step to ensure data is permanently erased involves adapting erasure methods to cover all types of data storage, regardless of the device. As storage devices are integrated into a wide variety of hardware, this approach ensures that data is securely and completely removed across all systems.

Secure data erasure guarantees that data cannot be recovered by any means, in line with data protection laws.



INTRODUCING CERTUS ERASURE

For many years, Certus has been at the forefront of secure data erasure technology. We design, manufacture, implement and manage solutions that give users the platform to securely wipe data from all devices. We have wiped data from more than 350 million devices to date, making sure that data is erased permanently and securely, every time.

Our Certus Erasure software is designed to meet the highest industry standards for data erasure and data privacy compliance, including GDPR, NIST SP 800-88, and IEEE 2883-2022.

Certus Erasure gives users the tools to erase data from all devices and verify data erasure, with detailed, tamper-proof erasure reports which serve as an official record of permanent data erasure.

CONTINUOUS IMPROVEMENT

One of the most important things with data erasure software is to ensure continuous improvement, not only to support the latest technologies entering the market but also to make the process easier to use while ensuring more controlled and secure solutions.

Our latest improvement integrates the erasure software directly into a customer's internal network or third-party asset management applications. This allows data erasure to be triggered remotely, eliminating the need for manual intervention. Whether it's a PC or laptop, the software automatically erases data and generates evidence for compliance, making the process secure, efficient, and effortless for the customer.

GET IN TOUCH

For more information, to speak with our team, or to book your free trial visit www.certus.software.

We encourage organizations to get in touch and we'd be more than happy to guide you through the erasure process.

