Privia SECURITY

Data Sanitization Service

Professional Forensic Services

"Secure Data Erasure to DoD Standards!"

The information contained in this document pertains to the Forensic Services performed by Privia Security Information Technology and Consultancy Services Inc. and is of a **general** nature. All information in this document is publicly available.

Queen Elizabeth Olympic Park, 14 East Bay Lane, Plexal, London, England, UK, E20 3BS

info@priviasecurity.co.uk

www.priviasecurity.co.uk

"Secure Data Erasure Service is carried out in compliance with military data-erasure protocols such as the U.S. Department of Defense's DoD 5220.22-M standard. Military protocols guarantee that data is irrecoverably destroyed."

The Secure Data Erasure Service ensures that data is permanently erased in accordance with legal regulations and security standards. Organizations require this service to safeguard sensitive information stored on disk surfaces. Permanently deleting data minimizes the risks of information leaks and unauthorized access, thereby strengthening internal security.

Today, simply deleting data from a disk surface is insufficient because many deletion processes leave data recoverable. The Secure Data Erasure Service employs various techniques to render data irretrievable. These techniques include software-based data wiping, magnetic degaussing and physical destruction methods. Each method is carefully selected and applied to ensure that sensitive data is completely annihilated. Securely erasing data also plays a critical role in legal compliance. Particularly to meet regulations related to personal data protection and privacy, data must be securely destroyed. By complying with national and international regulations—such as the Digital Transformation Office's Information and Communication Security Directive—this service helps prevent potential legal risks.

Failing to securely erase personal or corporate information can lead to both financial and reputational damage. If confidential data is recovered and misused, an organization's reputation may suffer and trust may be lost. The Secure Data Erasure Service is an essential offering that ensures the security of sensitive information and establishes a safe data-management process. Permanently destroying data is one of the cornerstones of information security, making data management safe for corporate users.

Service Components

Software-Based Data Wiping

The software-based data-wiping method securely deletes data through specialized software. Custom-developed applications overwrite the data multiple times with random patterns, making recovery impossible. Software-based erasure is especially effective when securely deleting a large number of files. Data wiped by this method leaves no trace, thereby minimizing the risk of data leakage. It is commonly used for storage media such as hard drives and SSDs.

Physical Destruction Methods

Physical destruction involves permanently destroying the devices that store data. In this process, storage units—such as hard disks, SSDs and CDs—are shredded into small fragments so that data recovery becomes impossible. This method is preferred when it is critical to ensure that extremely sensitive data is completely secured.

Magnetic Degaussing

The degaussing method erases data by applying a strong magnetic field to storage media. In this process, high-powered magnets disrupt and eliminate the magnetic information on disks where data is stored. Degaussing is a highly effective method for permanently erasing data from magnetic storage devices. After degaussing, the data cannot be recovered.

SSD Data Erasure Protocols

Data erasure on SSDs uses special protocols because SSD architecture differs from that of traditional hard drives. On SSDs, data is stored via electrical charges in cells, so conventional methods are insufficient. The specialized protocols ensure that data on the SSD is permanently destroyed and that the device is made secure. Using dedicated software or hardware, all data residing on the SSD is securely wiped.

Cloud Data Erasure

Cloud data erasure ensures that data stored in cloud environments is securely deleted. Cloud providers implement various protocols to permanently remove data upon user request. Once erased, the data is completely removed from the cloud storage and cannot be recovered.

Encryption-Based Erasure

The encryption-based erasure method involves first encrypting data with strong algorithms and then deleting it. This approach ensures that even if the data is intercepted before deletion, it remains unreadable. Encryption provides an additional layer of protection for highly sensitive information. By encrypting data prior to secure deletion, this method ensures that data is irrecoverable.

FAQ

What is a secure data-erasure process and how is it performed?

Secure data erasure is the process of permanently destroying data so that it cannot be recovered. Unlike standard deletion operations, secure data-erasure methods overwrite data with random patterns or use magnetic fields to eradicate data, making recovery impossible. In environments containing sensitive information, secure data erasure is performed using specialized software or physical destruction techniques. Software-based secure erasure methods are typically applied to digital storage media such as hard drives and SSDs.

What is the difference between physical destruction and secure data erasure?

Physical destruction involves shredding the devices that store data into pieces. Secure data erasure, on the other hand, overwrites data multiple times so that it cannot be retrieved. Physical destruction renders devices unusable, while software-based secure erasure allows devices to remain functional. Physical destruction—such as degaussing or shredding—is preferred when the stored data is extremely sensitive. Both methods address different needs: physical destruction for absolute media disposal and software-based erasure for reusable devices.

Which devices can undergo secure data erasure?

Hard disk drives, solid-state drives (SSDs), USB flash drives and mobile devices can all undergo secure data erasure. Data stored in cloud systems can also be securely deleted. The methods used vary according to device type. For example, SSDs require specialized erasure protocols, which differ from those used on mechanical hard drives. Each device is rendered irrecoverable using techniques tailored to its characteristics.

How is secure data erasure related to legal requirements?

Secure data erasure is a critical requirement for compliance with national and international regulations—such as Turkey's KVKK, GİB, the EU's GDPR and NATO standards. Legal regulations mandate that sensitive and personal data be securely destroyed. If data cannot be securely erased, organizations may face serious legal penalties. Secure data erasure methods fulfill these requirements and ensure legal compliance.

How is the security of data-erasure software ensured?

Data-erasure software operates on specially developed algorithms to overwrite data in an irreversible manner. Many secure data-erasure tools are developed according to security standards such as the U.S. Department of Defense's DoD 5220.22-M. To ensure these tools are used correctly, users should receive proper training and periodic audits of the software's security should be conducted. Secure data-erasure software enables users to permanently destroy data, providing a reliable data-disposal process.

How long does the secure data-erasure process take?

The duration of secure data erasure depends on the volume of data to be erased and the method used. Small files of a few megabytes can be wiped quickly, whereas securely cleaning an entire drive may take several hours. Physical destruction methods generally have shorter turnaround times, while software-based overwrite cycles can take longer—depending on disk size and structure. Because verification is required after the erasure to ensure data security, the process may extend from several hours to several days.

Why is it not recommended to erase data without first backing it up?

Since secure data erasure permanently destroys data, it is essential to back up important files beforehand. Critical business files should be stored on an external device or separate system before erasure. Without a backup, losing essential data could cause significant damage. Because secure erasure is irreversible, backup needs must always be considered.

Can physically destroyed data be recovered?

No. Data that has been physically destroyed—whether by shredding devices or erasing with magnetic fields—cannot be recovered. Physical destruction renders devices completely unusable, ensuring that data retrieval is impossible. For storage media containing critical information, physical destruction is recommended. Methods such as degaussing use magnetic fields to thoroughly erase data, providing guaranteed security. Once physically destroyed, the device is disposed of and cannot be reused.

Does restoring factory settings replace the need for secure data erasure?

Restoring factory settings removes most user data but does not fully prevent recovery by forensic tools. Factory resets only clear surface-level data and remnants of sensitive or important files may remain on the device. Secure data erasure methods fully eliminate data so that it cannot be retrieved. To ensure data security, secure data erasure should be used instead of relying solely on factory resets. These methods completely cleanse the device and reduce the risk of data leakage.

Is it possible to recover data after secure data erasure?

No. Secure data erasure methods—such as multiple overwrite passes, magnetic degaussing, or physical destruction—make data recovery impossible. While data deleted by standard methods can sometimes be restored with specialized software, secure data erasure eliminates that risk. Once data is permanently deleted, no recovery software or technique can retrieve it.

Your Trusted Partner in Cybersecurity

Founded in 2018 with a vision for the future of cybersecurity, Privia Security has been committed to delivering high-quality services to its clients from day one. With a strong and capable team, we provide the most reliable and comprehensive solutions across all areas of cybersecurity, ensuring our clients are well-protected in today's digital landscape.

As cyber threats continue to evolve rapidly and grow in complexity, combating them becomes increasingly challenging. At Privia Security, we offer both defensive and offensive cybersecurity strategies powered by cutting-edge technology to meet our clients' evolving needs. Through our innovative R&D products and strategic consultancy, we aim to enhance organizations' cybersecurity maturity and deliver proactive, tailored solutions. We are proud to be safeguarding the digital assets of more than 300 major organizations.

Global and Local Cybersecurity Solutions

Privia Security delivers cybersecurity services across a broad geographical scope, including Europe, Asia, the Middle East and the Americas. Our specialized teams in Offensive, Defensive and Forensic operations develop bespoke solutions for organizations operating in diverse sectors such as critical infrastructure, avionics systems, corporate networks and the military.

In addition, our innovative cyber warfare simulation platform, PriviaHub, offers comprehensive solutions for nations seeking to strengthen their cyber defense capabilities. PriviaHub enables the testing of cyber warfare strategies, execution of simulations and assessment of expert competencies. Designed to meet the exercise needs of private sector entities, academic institutions and military organizations, it bridges the gap between training and real-world readiness.

A Secure Future Through Advanced Technology

With R&D centers located in Istanbul, Ankara, London and at Cumhuriyet Technopark, we are continuously developing value-driven projects for our clients. From penetration tests and red team operations to cybersecurity training and custom enterprise solutions, we are redefining the standards in our industry. Through our slogan "**Privacy For You**" we bring a fresh, innovative perspective to security and privacy—ensuring that our clients' digital futures are secure.

Privia
SECURITY