ASSET SCIENCE

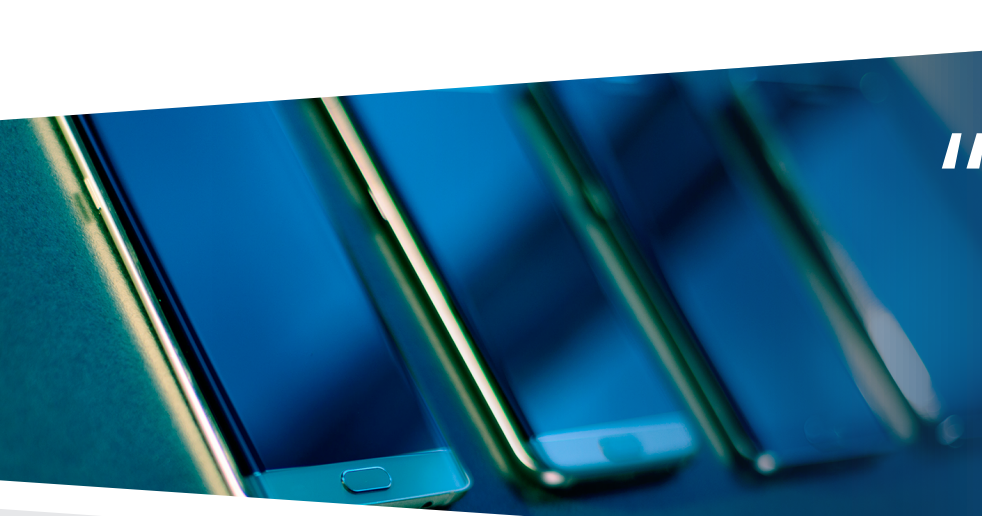
DATA ERASURE

Getting to grips with Data Erasure

A Beginner's Guide

> Data Erasure is a software-based method used to make inaccessible all user information and electronic footprint storage on mobile devices by overwriting free disk space or by throwing away the encryption key so that it renders the data effectively unrecoverable.

Page 6



> Data protection refers to the practices and binding rules put in place to protect your personal information.

Page 3

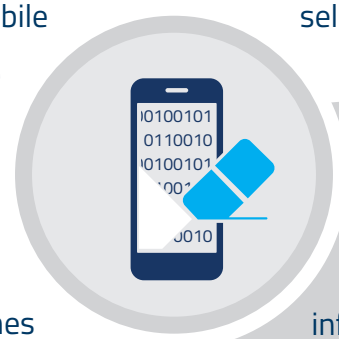
Table of contents

Are you targeting the secondary device market? Do you work with wireless carriers, buyback providers or repair shops? Does your business help facilitate the mobile device lifecycle?

If you answered **yes** to any of these questions, you are potentially dealing with sensitive personal data. From pictures to passwords, consumer information could still be on the smartphones you are processing. Mobile retailers, resellers and repairers need to securely erase mobile phone data, whether those devices are destined for recycling or resale.

But how do you know whether your current measures are sufficient, or if your company is exposing itself to fines and disgruntled customers?

This whitepaper aims to explain how you can protect yourself and your company by ensuring that you're using the most accurate and effective method available. Firstly, we'll explain why data privacy is such a hot button issue. We'll help you understand when, where and why Data Erasure should take place, and how it differs from other methods. Finally, we'll share some tips on how to select a supplier.



Data protection refers to the practices and binding rules put in place to protect your personal information and ensure that you remain in control of it. The individual decides whether or not they want to share information and who has access to it.

Why Data Protection is hot news:

Data protection is a serious matter. Privacy and cybersecurity are top of mind concerns nowadays. Consumers are worried about who has access to their personal information and companies are concerned about the **financial** and PR **repercussions** of a data breach.

Not clearing data from devices that are intended to be resold, recycled or discarded might end in severe reputational damage with financial and legal consequences, including **heavy fines** for breaking industry and government regulations.

GDPR: Securing personal information as a mandate

In May 2018, the **General Data Protection Regulation (GDPR)** came into effect. It regulates how companies protect and secure European Union citizens' personal data. However, the repercussions affect companies outside of the European Union also. Anyone who does business, or requests information from EU users, must comply with GDPR.

GDPR's vast and complex **rules** and **regulations** cover technology, laws, finance and ethics. All **wireless retailers, resellers** and **repairers** must fulfil the mandate of protecting consumer data on the devices in their possession.

Penalties are based on the volume of data compromised and the level of the company misconduct. Fines could go up to 20 million Euros or 4% of annual revenues, whichever is greater.

Looking ahead

The North American market should expect new data regulations progressively coming into force in the near future. Complying with GDPR is a way of preparing for the regulations states like California and Alabama are already implementing.

Find out more:
https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations_en

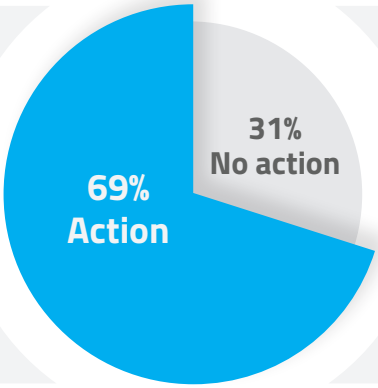
Attitudes to data privacy

It's not just national or regional governments that are acting: **individual users** have increasing expectations of **data privacy**. And when those expectations are thwarted, the consequences can go beyond one unhappy customer.

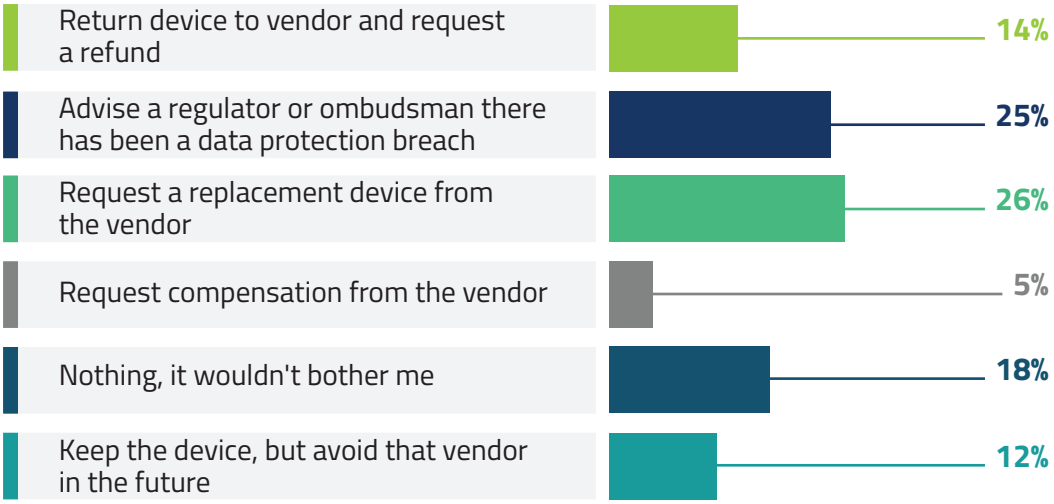
We recently **conducted a survey** in the United States to understand customer reactions to data privacy breaches. The results were clear: many customers **wouldn't hesitate** to make **a formal complaint** to regulatory bodies, as well as requesting individual compensation.

We asked respondents what action they would take if a second-hand device they had purchased turned out to have data on it from the previous owner.

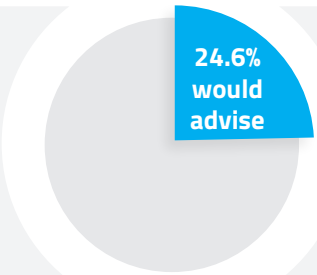
69% of the participants responded that they would be sufficiently unhappy to **take some action**, such as returning the device, demanding a replacement, asking for compensation or even **escalating the issue** to a regulator. Even amongst those who would keep the device, 12% stated that they would avoid the supplier in future.



If you discovered personal data from a previous owner on a second-hand device, which of the following actions would you take?



What's more, the survey revealed an interesting tendency. **A quarter** (24.6%) of the respondents would be willing to **advise a regulator** or ombudsman that there has been a **data protection breach**. This could lead to an investigation that can easily end in fines and reputational damage.



Another interesting insight from the survey is that Apple users are more likely to react negatively, with 27% stating that they would "Return device and request a refund" as opposed to only 4.44% of Android users.

Sample: 241 American adults who own a mobile device.
Online Survey conducted by Asset Science in August 2018

Data Erasure on mobile devices

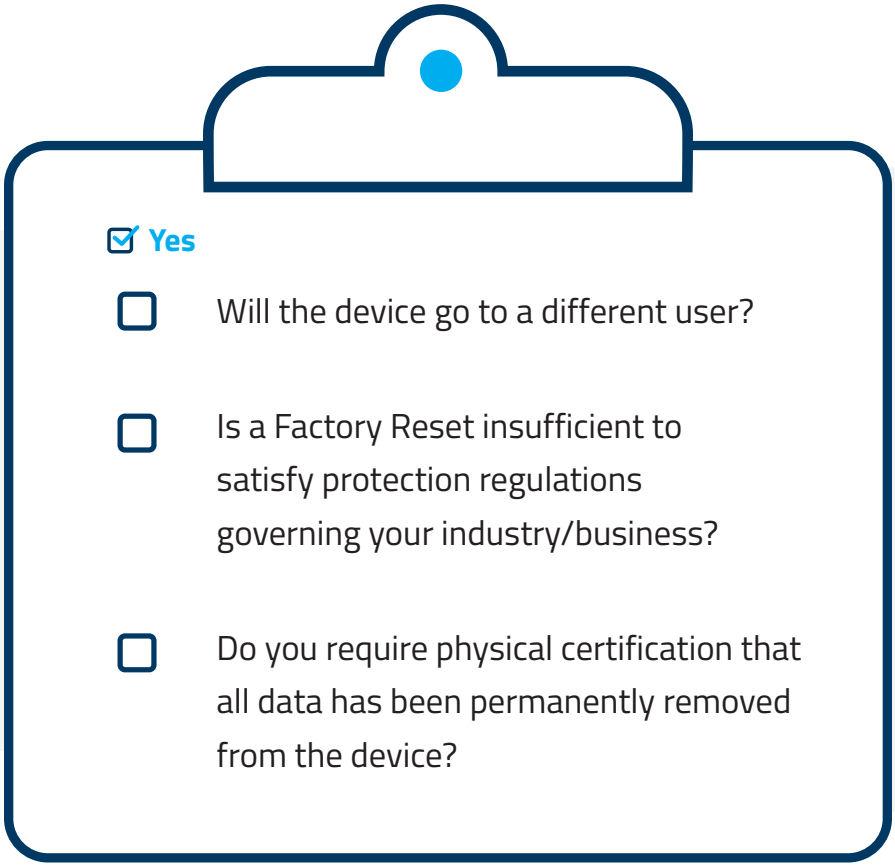
Data Erasure is a **software-based method** used to make inaccessible all user information and electronic footprint storage on mobile devices by overwriting free disk space or by throwing away the encryption key so that it renders the data effectively unrecoverable.

When is Data Erasure necessary?

Data Erasure is a process that goes beyond basic file deletion, which only removes direct pointers to the data, making it still potentially accessible with software tools. So, in order to protect privacy and personal information, **Data Erasure** should be the standard when disposing, recycling, exchanging or reselling a fleet of devices.

Checklist

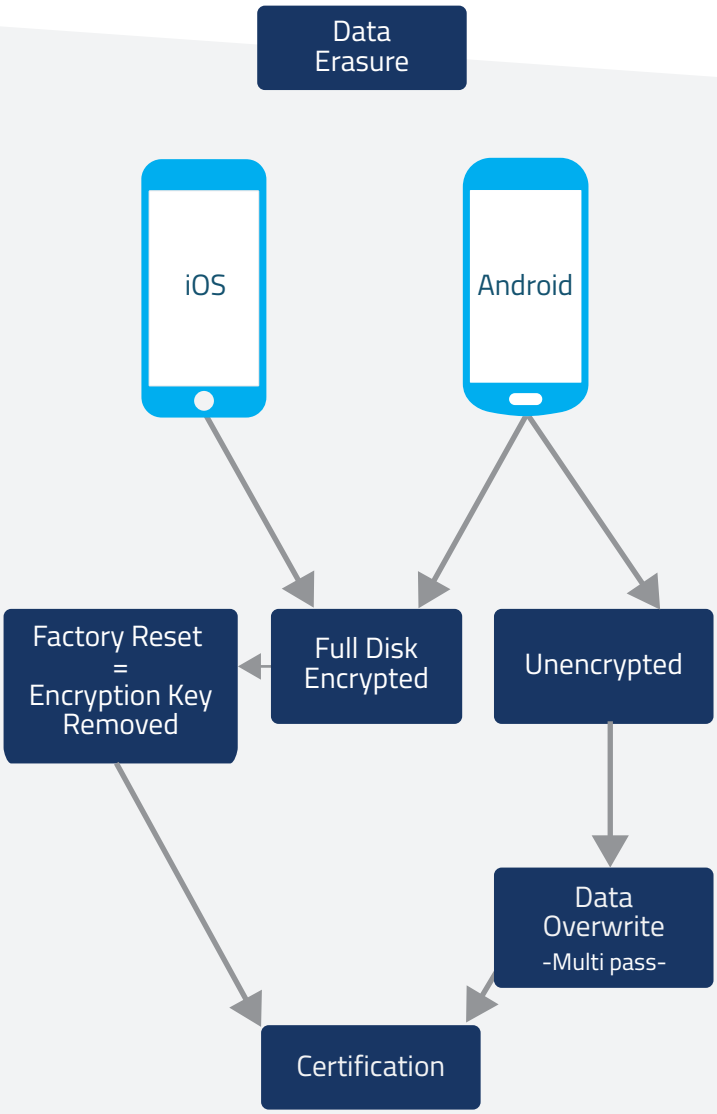
To guarantee you don't put any personal or corporate data at risk, review the following checklist to identify whether a Data Erasure procedure should be part of your process.



If you answered **yes** to one or more of these items, you should consider performing full data erasure.

How is it done?

Even if the outcome is the same, the procedure varies from iOS to Android devices.



For Apple iOS

- Apple's iOS devices, including iPhones, use a full encryption system.
- By applying an iOS factory reset the encryption keys are erased and this makes any data left on the device unreadable.
- Once the device switches to Activation Mode, flashing is complete, and all data becomes inaccessible. System is restored with the latest iOS version available.

For Android

- The Android operating system can be either set to encrypted or unencrypted mode in most recent devices as of Android 6.
- To effectively erase data on an Android device, it is necessary to first detect the type of encryption and then take the correct action to remove it.
- For Android unencrypted devices, completing a factory reset is not enough, so it's necessary to perform a complete overwrite. When this procedure is completed the phone is restored with the same OS version it previously had.

The security goal of the overwriting process is to replace target data with non-sensitive data.

DELETION vs. ERASURE

Deletion and Erasure sound similar but there is a technical distinction between them. If data is deleted it could still be recoverable, but if it is effectively erased it is not.

Data Erasure is an auditable and certifiable method.

Erasure

Process intended to render stored information irretrievable by normal means. Also known as wiping or shredding files.

Delete

A temporary way of removing items. Deleted items are still available for restoration since only the pointers to the physical location have been removed.

Media Sanitization

A general term for the actions taken either to irreversibly remove data from a media or its physical destruction.

What about ENCRYPTION?

Encryption is the process of encoding information in such a way that only authorized parties can access it. Encryption is a technical procedure to secure data either when it is transferred or when it is stored on the device.

There are different levels of encryption, but some can be unlocked with the matching key. With current decryption technologies, losing or erasing the key makes the data effectively unrecoverable.

FACTORY RESET vs DATA ERASURE

A **Factory Reset** brings the device back to its original settings to improve the performance and in many cases will still retain some data. Recommended when the device is not changing hands.

A **Mobile Data Erasure** overwrites all data until it becomes fully unrecoverable. It should be done when devices are exchanging hands.

If the device is potentially changing hands, a factory reset may not be enough.

Choosing a supplier:

Look for an organisation that is accredited by a credible 3rd party, such as ADISA.

ADISA (Asset Disposal Information Security Alliance) is an organization, based in the UK, that certifies to the highest standard for Data Erasure.
After extensive evaluation and testing, **ADISA** endorse the procedure applied by companies doing Data Erasure guaranteeing that all user data is cleared without compromising privacy and following industry and government regulations.

Other standards that are also worth looking out for are Kroll Ontrack and compliance with the U.S. National Institute of Standards. Different certifications are available on the market for other types of devices like laptops and tablets, but don't be misled by the number of certifications some companies claim: check that they are directly related to mobile devices.

Why Asset Science?

Asset Science has been a leader in the mobile device diagnostics industry since 2010. We work with OEMs, wireless carriers, buyback and insurance appraisers, and reverse logistics factories to improve testing accuracy and boost customer satisfaction.

Trustworthy solution

- Erase with confidence thanks to ADISA certification.
- Improve processing times and increase operational efficiency.
- Expertise in OEM-Level mobile device testing and diagnostics.

An Integrated solution

- Convenience of having one trustworthy supplier for Diagnostics and Data Erasure as an end to end solution.
- One familiar and accessible interface for the operator.

Audit & Accountability

- Keep track of your inventory for regulatory compliance.
- A flexible solution that works from startups to multinationals.
- Individual/batch or device certification allowing you to prove device condition.

Get in touch
assetscience.com
info@assetscience.com
US/Can toll free: 1-866-ASCI-101