

DATA ERASURE & RECYCLING

Overview

Data Erasure Methods

Destruction and Recycling UK



Corporate Mobile Recycling Ltd

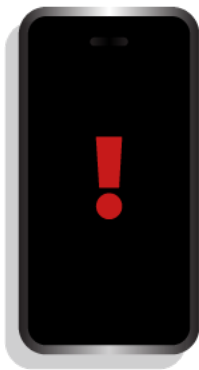
Overview

In accordance with the General Data Protection Regulation (GDPR), businesses need to consider any personal data that an employee may have saved on work mobile phones and other devices as well as potential customer data.

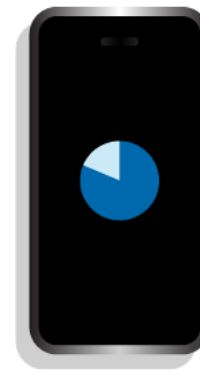
Data stored on these devices can range from photos, text messages, personal emails, all of which would be considered as identifiable data under GDPR. This essentially means that any company mobile phones could fall under the requirements of GDPR.

As market leaders in mobile device trade-in, CMR have developed a robust, certified data erasure process to ensure that all customers can be confident of compliance to GDPR and other data protection regulations.

CMR's Data Erasure Service is integral to the business' processing. Using Piceasoft for Mobile Devices and Global Erasure for Macs, devices are erased and certified by reports ensuring that you can provide the necessary evidence to any regulator or auditor quickly and easily.



Devices arrive via potentially containing sensitive data



Industry leading software permanently removes data



All data is removed from the devices beyond recovery



Certified reports provide assurance

Data Erasure: Piceasoft

CMR's Data Erasure Processes

Piceasoft is CMR's mobile phone and tablet data erasure software.

It allows CMR to perform a Cryptographic sanitization on each mobile phone or tablet.

Piceasoft certificates are generated for each device erased as part of CMR's quote reporting.



Manual Data Erasure (Older devices not compatible with the third-Party Data Erasure Tool)

Data is erased by our team manually by carrying out a full factory reset on the Mobile Device in line with the manufacturers recommended guidelines. We have comprehensive controls in built into our system ensuring that the data wiping is completed and have full audit trail of when the data erasure took place along with the individual that completed it. Manual Data Erasure Certificates are generated by our system for every Mobile Device going through this process.





Data Erasure Report

Report Details

Name	
Order Number	20059
Report id	359b90f8-5642-4ed1-a916-46d5527d9d35
Created	08/02/2024 11:28:43
Product	PiceaEraser 2024.1.1.33

Source Device

Manufacturer	Apple
Model	iPhone 11
IMEI	3 48833
Serial Number	FFWH7H3YN7J
Operating System	16.6
Internal Storage	64GB

Erasure Details

Erasure Method	Cryptographic sanitization
Duration	307 secs
Result	DP_OK

I hereby state that the data erasure process has been carried out in accordance with the given instructions

Supervisor

External Data or Sim cards found with devices will be shredded as part of the data erasure process.

Any external labels stuck to or attached to devices will be removed and destroyed as part of the data erasure process.

PiceaEraser regulation compliance

This report is subject to Piceasoft EULA: <https://services.piceasoft.com/index.php/eula?lang=en>

EUROPEAN UNION: Erasure done in accordance with REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [Document 52012PC0011].

PiceaEraser is designed to meet and exceed requirements set in Article 17 'Right to be forgotten and to erasure' <http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52012PC0011>

UNITED STATES: Mobile data media sanitation in compliance with NIST SP 800-88 rev 1 <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf>

Followed Cryptographic Erase Guidelines which is conformance tested for FIPS 140-2. Modules validated as conforming to FIPS 140-1 and FIPS 140-2 are accepted by the Federal Agencies of EU and US for the protection of sensitive information <http://csrc.nist.gov/groups/STM/cmvp/>

GENERAL: Administrative/Privacy/Security policies in ISO 27001, PCI DSS, HIPAA and SOX require secure data removal. PiceaEraser ensures regulatory compliance with data destruction, reporting and auditing capabilities.



Piceasoft

Report id: 359b90f8-5642-4ed1-a916-46d5527d9d35

Manual Data Erasure Report

This DataWipe report has been generated for CMR Limited and confirms that all user data on the device detailed here under has been successfully removed beyond realistic recovery. External Data or SIM cards found with devices will be shredded as part of the data erasure process.

CUSTOMER INFORMATION

End Customer:

REPORT INFORMATION

Order number: 20059
Report Date: 22/02/2024 12:19:59
Data Erasure Method: Manual

DATAWIPE INFORMATION

Data Erasure Status (Pass/Fail): Pass
Duration: 05 min 16 sec
Removable Memory: n/a
SIM: n/a

DEVICE INFORMATION

IMEI:
Internal Registration ID: 100112173
Device Make & Model: Apple iPhone 11 64GB
Operator Name: Nazret@cmrecycling.co.uk
Supervisor: Jonathan Russell
Date & Time Erasure: 08/02/2024 12:22:57

I confirm that the DataWipe has been executed successfully



Signed by Manager

3 Long Yard • Holborn • London • WC1N 3LS. Registered in England no. 4591053 VAT No. GB 915 7847 89

Data Erasure: Global Erasure

Global Erasure provide CMR's Mac data erasure software. Global Erasure performs a thorough erasure exceeding the NIST Purge level. The software is able to erase all models including M1 and M2 chips. Each erasure generates a certificate in our system. These can then be sent to our clients for proof of erasure.

Global Erasure powered by YouWipe is a software-based method, ensuring that 100% all data on HDD, SSD, Flash and Mobile devices is completely destroyed and rendered unrecoverable by any current technology. YouWipe has been certified under rigorous and professional standards, by governments and independent security organizations, such as NATO, the UK National Cyber Security Centre (NCSC), the Common Criteria (EAL +3), the Dutch General Intelligence and Security Service, the Finnish National Cyber Security Centre (TRAFICOM), and ADISA (UK Asset Disposal and Information Security Alliance), among others. Global Erasure meets and exceeds strict government regulations and industry standards, such as the GDPR, HIPAA, FACTA, PCI DSS, SOx and the Data Protection Act. Once a disk is erased, a digitally signed, tamper-proof certificate of erasure provides a detailed audit trail to comply with external or internal auditing requirements.



Global Erasure Certificate

Erasure Report

2023-11-15 / 13:12

TD SYNnex | **Renew**

Organization

TD SYNnex Renew

Operator

Operator

C02TQ71HHV2M

NVMe / APPLE SSD AP0512J

Erasure success *

Vendor / Model	NVMe / APPLE SSD AP0512J	Erasure level achieved	Baseline security
Serial number	C02721200VKHRR311	Erasure standard	NIST.SP.800/ATA Purge
Type	SSD	Erasure passes	3
Command protocol	ATA	Erased sectors	100% (122138133)
Transport	NVME	Verified sectors	10% (12213810)
Size	500.3GB	Erasure started	2023-11-15 13:00
Size (bytes)	500277792768	Erasure time	11m 21s
Sectors	122138133	Errors	0
Sector size (bytes)	4096	Secure Erase	Not Attempted, Time estimation not found
Remapped sectors	0	NVME Format	Not Attempted, Time estimation not found
HPA	Not supported		
DCO	Not supported		

(*) All user accessible areas have been erased successfully. Disk may contain user inaccessible areas which are primarily used by hardware vendors to store system or defective information. In case these areas are also required to be erased, use extended erasure standards or contact our support for more help.

Report Details

Report signature	Verified	Project
Report tag	C02TQ71HHV2M	Contact person
Report date	2023-11-15 13:12	Location
Report ID	859430c8-def3-45fc-b47f-978df1c9e2ab	Department
Session ID	fe6fd2ae-f997-482e-b177-155630046738	Branch
Erasure software	GlobalErasure 4.1.257.2309131038-90bfe4fe	

Hardware Details

Model	MacBookPro14,2
Serial number	C02TQ71HHV2M
Processor	GenuineIntel,Intel(R) Core(TM) i5-7267U CPU @ 3.10GHz,x86_64 @ 3.5GHz, logical CPUs: 4, Speed: 3500MHz
Battery Info	Vendor: SMP,Model: bq20z451, Serial: , Type: lithium-ion, Capacity: Some(87)%, Voltage: Some(12.0) V
Battery Test	Battery health OK
Memory	8GiB
VGA compatible controller	Intel Corporation Iris Plus Graphics 650
Network controller	Broadcom Inc. and subsidiaries BCM43602 802.11ac Wireless LAN SoC
Audio device	Intel Corporation Sunrise Point-LP HD Audio

Operator:

Supervisor:

GlobalErasure 4.1.257

Recycling/Destruction

CMR has partnered with **Restore Technology** to provide destruction and recycling of any devices that failed to data erase. We consolidate our devices for a monthly pickup from Restore Technology.

Restore Technology is UK government-approved to handle and destroy protectively marked media up to the highest UK security level, they can carry out this service at scale at either their own facilities or on our sites.

The service includes full reporting, ensuring every single asset is tracked and accounted for, and certificates of destruction are also provided.

Data shredding

Restore Technology's CPNI and NCSC-approved destruction service includes hard drive shredding – They are capable of shredding down to 2mm, as required. The service includes the scanning of hard-drive serial numbers prior to shredding on site, ensuring a complete audit trail of secure data destruction.

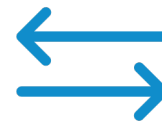
Data degaussing

Restore Technology's degaussing machines use a powerful magnetic force to destroy the data on the processed devices.



Ultra-secure

Restore Technology are approved to destroy data to the maximum UK security level, and they can meet any destruction policy worldwide.



Tracked

Our equipment will be tracked through the entire process, and a full destruction report for all assets will be provided once complete.



Sustainable

Their recycling processes involve segregating assets into their waste streams before they are sent to vetted, specialized downstream waste partners for material reclamation.



Compliant

Their services are compliant with all security and environmental standards, giving us complete peace of mind.

Recycling/Destruction Certificate



Data Destruction and Recycling Report

This report has been generated by CMR Limited and confirms that the device's data will be destroyed and recycled. External Data or SIM cards found with devices will be shredded as part of the data erasure process.

CUSTOMER INFORMATION

End Customer: Tech Data

REPORT INFORMATION

Order number: 18788
Report Date: 19/01/2024 14:31:14
Data Erasure Method: Destruction

DATAWIPE INFORMATION

Data Erasure Status (Pass/Fail): FAIL
Removable Memory: n/a
SIM: n/a

DEVICE INFORMATION

IMEI: C02D32V0ML7H
Internal Registration ID: 100111187
Device Make & Model: Apple MacBook Pro Core i5 A2251 13 2.0GHz 16GB 512GB 20
Operator Name: kasia@cmr.com
Supervisor: Jonathan Russell

I confirm that the device will be sent to CMR's secure and accredited destruction partner, Restore Technology. All device components will be destroyed & recycled. Devices are sent periodically, CMR receive certification upon completion of this process.

Signed by Manager

3 Long Yard • Holborn • London • WC1N 3LS. Registered in England no. 4591053 VAT No. GB 915 7847 89

CMR Security Measures

Our facility is a certified Transport Asset Protection Association (TAPA), and a Facility Security Requirements (FSR) level A site which is the highest standard. Many security measures are put in place such as 24/7 CCTV covering all the building and every workstation. Security guards and full body scanners are used for every members of staff coming in and out the building.

The FSR Standard is reviewed independently every 3 years but audited every year in between consultation with the Association's members to ensure its effectiveness and efficiency. For TD SYNEX EMEA, this is a mandatory standard and certification.

We are proud to report that our building security exceeds the FSR standard.

