GDPR & DATA ERASURE

Contact Olly Tagg
Tel +44 (0)207 404 6440
email ot@cmrecycling.co.uk
www.cmrecycling.co.uk

Corporate Mobile Recycling Ltd

GDPR & DATA ERASURE

Today's mobile devices store a wealth of personal, confidential and sensitive data:

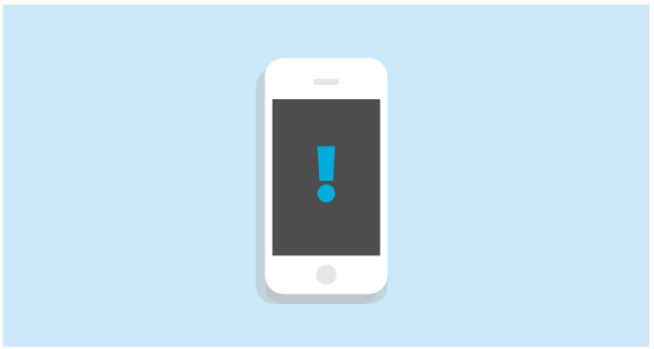
- Accounts, financial details, client and employee documents
- Contact details, activity history, call/SMS logs, GPS fingerprint
- Social networks, video, photo and other media files

Factory reset or software flashing will only remove data at user level. Smartphones are fitted with a complex flash memory (to prolong device memory) rendering Magnetic Erasure methods ineffective. Both methods can be exploited relatively easily by using commercially available forensic software.

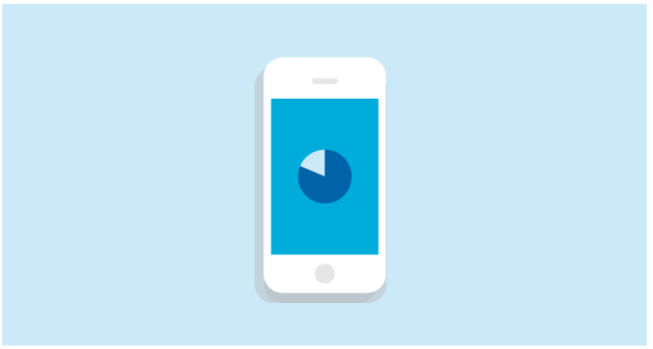
CMR's advanced Data Erasure Service is integral to the business' processing. Using Piceasoft, devices are erased and certified by reports. This mitigates risk for organisations in order to recycle devices with complete confidence and documented assurance.

CHECK POINTS

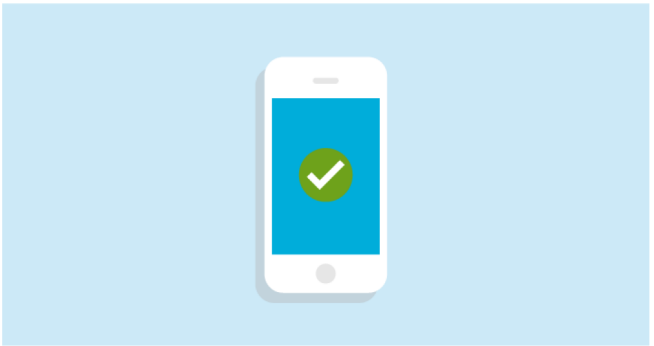
- All data removed beyond recovery
- Supports; Apple iOS, BlackBerry, Google Android, Symbian, Windows Mobile
- Certified Reporting



Devices arrive, potentially containing sensitive data



Industry leading software permanently removes data



All data is removed from the devices beyond recovery

Certified reports provide assurance

Corporate Mobile Recycling Ltd

GDPR & DATA ERASURE

INTRODUCTION

Increasingly, employees use, store and access personal data across a number of devices including personal and work mobile phones. With the introduction of General Data Protection Regulation (GDPR) in May 2018 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.

Employee personal 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 phone trade CMR have developed a robust and fully certified data erasure process to ensure that all customers trading in devices can be confident of compliance to GDPR and other data protection regulations. We provide data erasure certificates for every single device that we handle, ensuring that you can provide the necessary evidence to any regulator or auditor quickly and easily.

OUR DATA ERASURE PROCESS

SIM Cards & Memory Cards

Any SIM cards or memory cards will be removed from the Mobile Devices upon receipt and destroyed.

Mobile Devices

Data Erasure may be achieved by the following methods;

- third party data erasure tool
- manual data erasure
- destruction

Third Party Data Erasure Tool *(Most devices that we receive)*

Data is automatically erased by connecting a device to a third party data erasure tool such as Piceasoft or Blackbelt. Seamless integration between CMR systems and the third party tool ensures that certified Data Erasure Certificates are generated for each and every Mobile Device processed.

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.

Destruction (Non-functional devices)
For handsets that require destruction and recycling we use our long term partner Else Recycling and Refining (ERR).

- ERR follow the same procedures as CMR with equipment being logged in on arrival and allocated a consignment reference immediately. This enables assets to be tracked right through the process. Assets are protected by digital CCTV system and central station monitored intruder alarm. ERR's location is highly discreet and minimal signage is displayed.

- In the event of total destruction, ERR shred hard drives in a MeWa shredding system, which permanently destroys the drives, making data retrieval impossible.

- All magnetic tape media is shredded in a MeWa shredding system and then incinerated at an Energy from Waste facility. This is the most environmentally friendly method of recycling this sensitive product.

- Customer assets remain within ERR's domain until the data has been successfully purged 100% or the data carrying device has been destroyed. Assets are not consigned to any third party processors.

- The data destruction solution is approved to the highest CESG level with full audit and reporting provided as standard.

- Certification is provided for each device either through customer login access to the CMR processing portal or upon customer request