CCS Hard Drive Data Destruction Service

Assisting companies with GDPR Compliance

Contents

Introduction

The amount of data that companies process (knowingly, but also without realising) each day is increasing and shows no signs of slowing down.

The way that companies process data is diversifying. The days of talking, posting and faxing are all but gone, and these 'transactions' now take place in many different ways; from emailing, printing, photocopying and scanning, to online portals, document workflow solutions, and supply chains passing information back and forth manually & also automatically through various API integrations.

Additionally, the type of data that companies process is growing as advances in technology allow us to know, collect and share more information about individuals than ever before.

As a result new legislation is coming into force in May 2018, the European General Data Protection Regulations (GDPR), which will work side by side with the UK Data Protection Act 1998 (DPA).

These new regulations are not optional and apply to any company that process the personal data of individuals living within the EU, with big fines of up to 20 million Euros or 4% global turnover a real possibility for non-compliance.

The job of controlling who has access to an individual's personal data is by no means an easy one but the new regulations mean that now, more than ever, businesses need to recognise their responsibilities and put measures in place to fulfil their legal obligations when it comes to what happens to the data they hold.

One of the areas that is perhaps most overlooked when it comes to this is what happens to the personal data that is being held by a company when it is no longer required.

What happens to the contents on the Hard Drive of the old PC, laptop or photocopier that leaves your premises when it's either broken beyond repair or you've replaced it with the newer, faster, more current model?

Every photocopy, every document sent to print and every scan to email can be stored on the Hard Drive of a photocopier/ printer/multifunction device, and needs to be deleted in a secure manner. Hard Drives on older models have to be physically removed from the inner workings of the machine and disposed of by secure means. Newer models can be accessed and deleted from the control panel but only by an engineer, which is a problem for most companies who won't have a specially trained internal team able to do this.

From 25th May 2018, failure to manage this data properly will be in breach of GDPR regulations.

Solving this problem is the primary task of the new CCS Data Destruction Service. Specifically focused on the data held on the Hard Drive of these types of machines (Electrical and Electronic Equipment), we have teamed up with a specialist provider, who is compliant with HM Government & International Security and Environment Standards, to provide a secure disposal service to our clients.

Our mission is to assist our clients in demonstrating their GDPR compliance by taking away the pain of having to arrange the secure disposal of the Personal Data contained within their printers, photocopiers & multifunction devices.

Market Overview

The demand for multifunction devices is on the rise. Research firm, CCS Insight, predicts 124 million printers to be shipped worldwide in 2018, an increase from 106 million in 2013, with multifunction device sales increasing the most.*

*https://www.ccsinsight.com/press/company-news/1924-ccs-insight-launches-printer-and-mfp-forecast

Current problem

Awareness of the risk

A key area of the GDPR is that companies process personal data securely and the DPA is founded on a set of 8 principles, with principle 7 being:

> *"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."*

Most businesses, by completing internal reviews on process, infrastructure and who they share their date with, in the lead up to the GDPR enforcement date, may consider that they fully understand where their vulnerabilities are.

However, what most are probably not aware of is that there is a (at least one) silent and inconspicuous danger, which has huge GDPR implications, sitting right next to them in the office.

Any or every photocopy, document sent to print and scan to email may be, optionally, stored on the Hard Drive of a photocopier/ printer/multifunction device.

If you consider what a company will process through one of these machines – every business will have to perform HR function - personnel documents, drivers licence, passport information, medical information,

next of kin details, will all at some point go through the process of either being photocopied, printed or scanned to email.

In specific industry sectors – legal (solicitors), medical (doctors practice), education (school), additional personal data could include photos, criminal offence history, ethnic origin, religion, sexual orientation and so on.

All of the examples above are classified as 'special category data' by the GDPR, and it is considered that the breach of this type of information which would have a high impact on the rights and freedoms of the individual. The strongest penalties will be handed out to those who do not ensure this data is handled properly.

Hard Drives

The print industry continues to evolve along with the rest of the technology world and with that comes changes in the technical build and digital software abilities of the machines.

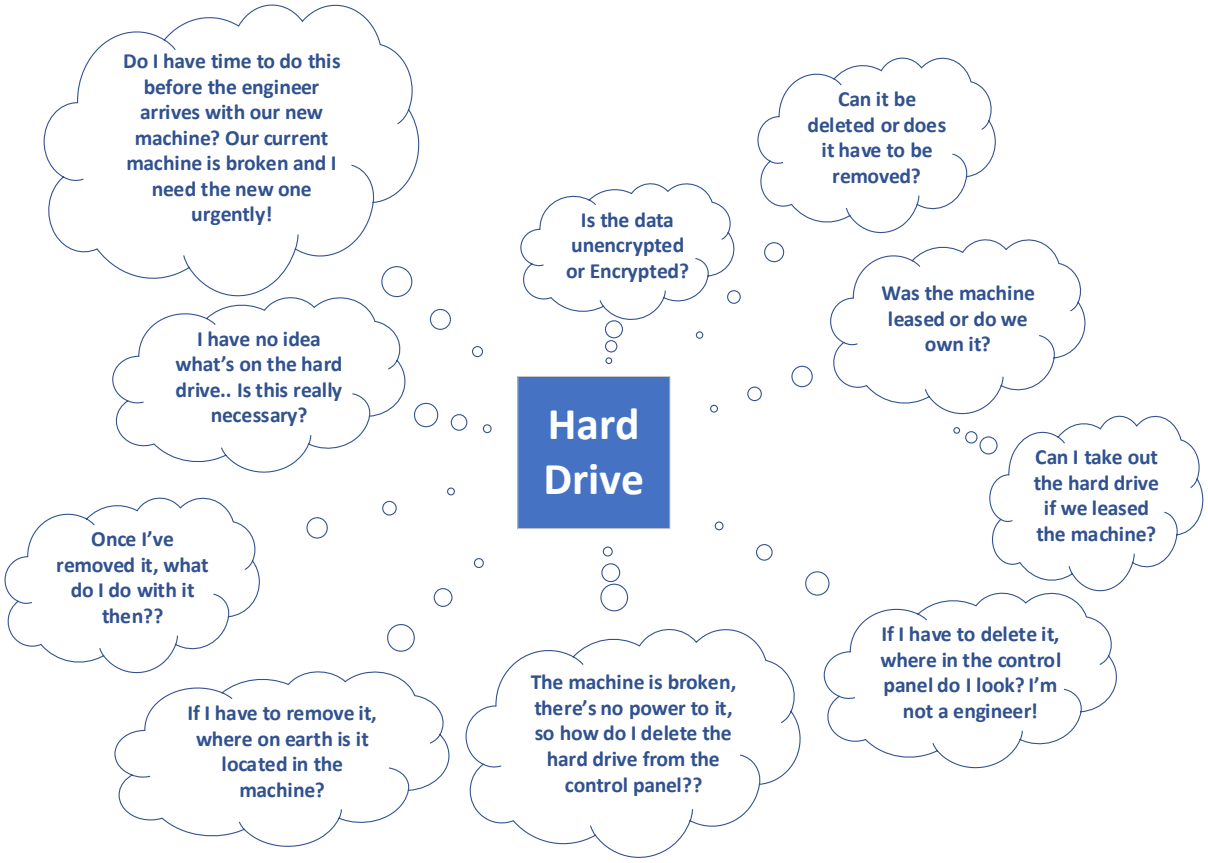
In the (not so distant) past, a majority of machines had a physical Hard Drive that was unencrypted and inaccessible via the control panel. These days the Hard Drives in a high proportion of the machines come automatically layered with encryption services that can be manager by an engineer.

When a photocopier is broken beyond repair or being upgraded/ replaced with the newer, faster, model, currently (in a vast majority of cases) the machine is swiftly removed from site, never to be seen again. The old/ broken machines are taken back to the supplier warehouse, where they're either recycled, resold, or dumped.

However, from 25th May, the owner of the data, i.e. the customer (the 'Controller' in GPDR terms) will be responsible for what happens to the data from creation all the way through to destruction.

Know How

But how does the Office Manager know where to start with regards to deleting the data? Many thoughts will no doubt be rushing through their mind –



Lack of resource or skill to fulfil your requirements does not absolve you of your obligations. The GDPR and the regulatory bodies are not concerned by the fact that your company does not have the time to give to this or a full time, on site photocopier engineer on hand to manage the data, or that you are unaware of what it is on the Hard Drive and therefore you're 'not sure' that the regulations apply.

The strongest force of the regulation will be applied to those who are negligent with 'special category data'.

CCS Solution

As a Print Management company, we specialise in the supply and service of photocopiers, printers and multifunction devices. It's what we do day in, day out – after all, it is our profession.

We understand the pain that is heading towards our clients, as we know the broad range and specifications of the machines out in the market - not just on sale today, but all the legacy machines out there too as these are covered under the GDPR regulations also.

Some months ago we realised that we were the solution to the problem.

Combining our knowledge of your equipment and a data disposal service provided by our partner, whose procedures (which are used for this service) are approved by the UK Ministry of Defence and are based on their original UK Government (CESG/ Cheltenham GCHQ) claims tested service, our solution offers the complete package in Hard Drive data destruction.

How it works

Your machine will be transported by a logistics company to our warehouse where it will be immediately stored in a secure part of the premises, which is only accessible by those members of CCS who need to in order to fulfil their duties (role based access) AND are trained to handle personal and Special Category data.

The machine will be processed in accordance with the type of Hard Drive that is contained within your machine.

The Common Criteria portal, which is not created or maintained by CCS, contains a list of all multifunction devices that contain encrypted Hard Drives - https://www.commoncriteriaportal.org/products/

This portal has been made available to support the information on the status of the CCRA (Common Criteria Recognition Arrangement), the CC (Common Criteria for Information Technology Security Evaluation) and the certification schemes, licensed laboratories and certified products.

All devices that are not contained in this list will have an Unencrypted Hard Drive.

Unencrypted Hard Drives

The Hard Drive will be removed, logged on a register and placed into a secure container. No members of CCS have access to the contents of the container.

The container will be collected by our data destruction partner, whose procedures are compliant with HM Government & International Security and Environment Standards, and securely transported to their facility adhering to the following standard of service:

- **MOD Security Cleared Drivers**
- **Uniformed staff carrying photo ID**
- **Unmarked vehicles**
- **Double manning (so one operative is always with the vehicle)**
- **Satellite tracking (with remote emergency vehicle disable)**
- **In built communications systems**
- **Triple skinned cargo stowage isolated from the drivers cab (vehicle outer skin, Inner cage bolted to vehicle floor, padlocked metal crate kept within, and chained to, the Inner Cage)**
- **Serial numbered security seals and tamper proof containers**

In addition to being compliant with the aforementioned standards, our chosen partner has a plethora of other credentials, demonstrating how committed to data security they, and CCS by association, are:

- **ISO 27001:2005 Information Security Management System**
- **ISO 14001:2004 Environmental Management System**
- **ISO 9001:2008 Quality Management System**
- **All necessary Environmental Agency and WEEE approvals.**

The destruction process will remove all data from the drive including operating systems. It is suitable for dismounted or loose Hard Drives as well as those mounted in servers, workstations, laptops, photocopiers, printers and multifunction devices.

The erasure software deployed is approved by CESG, the UK's Government Information Assurance Authority and the processes used are those specified in their original CESG/MOD approved service.

In a typical batch where devices/drives come directly from a working environment and are in good condition, up to approximately 5% of drives returned may be faulty or therefore cannot be safely overwritten. This is usually because they're no longer readable (fail to spin, have damaged power/cable connectors) or have faulty sectors. If a drive/device had a fault and cannot be overwritten it will be physically destroyed - again to CESG standards.

A report detailing the serial numbers of all the Hard Drives deleted will be produced and issued to CCS.

A certificate from our partner can be requested at the point you arrange for the collection of your device/s, for an additional charge.

Encrypted Hard Drives

The Hard Drive will be deleted via the machine Control Panel by one of our specially trained engineers and the Hard Drive details will be logged on our register.

Providing the Service

Corona Corporate Solutions is committed to assisting clients with their GDPR compliance, with respect to the destruction of data on their photocopier/ printer/ multifunction device. Therefore, this service is provided as part of the Agreement when a new machine is purchased.

Any client who wishes not to take this service with CCS is asked to sign a disclaimer, acknowledging and accepting the risk of the data they are responsible for being breached and the associated implications for non-compliance with GDPR and the DPA.

Disclaimer

Corona Corporate Solutions can assist with, but cannot guarantee, GDPR compliance for your company, based purely on this service.

Whilst we consider the steps above to be in accordance and compliant with GDPR regulations and the requirements placed upon you as part of the Data Protection Act 1998 with respect to the disposal of your IT Assets, we recommend you seek independent legal advice, as part of your due diligence, to verify this should you choose to rely on this service under compliance review by the ICO or any other regulatory body.