BLACKMORE RICOTECH

Your secure IT asset disposal experts

Secure IT Asset Disposal and GDPR

BLACKMORE RICOTECH is doing more to help you meet your GDPR compliance.

As a secure ITAD we're helping you to protect yourself – not only from ICO fines, but damage to your reputation if you fail to "do enough to protect" your data.
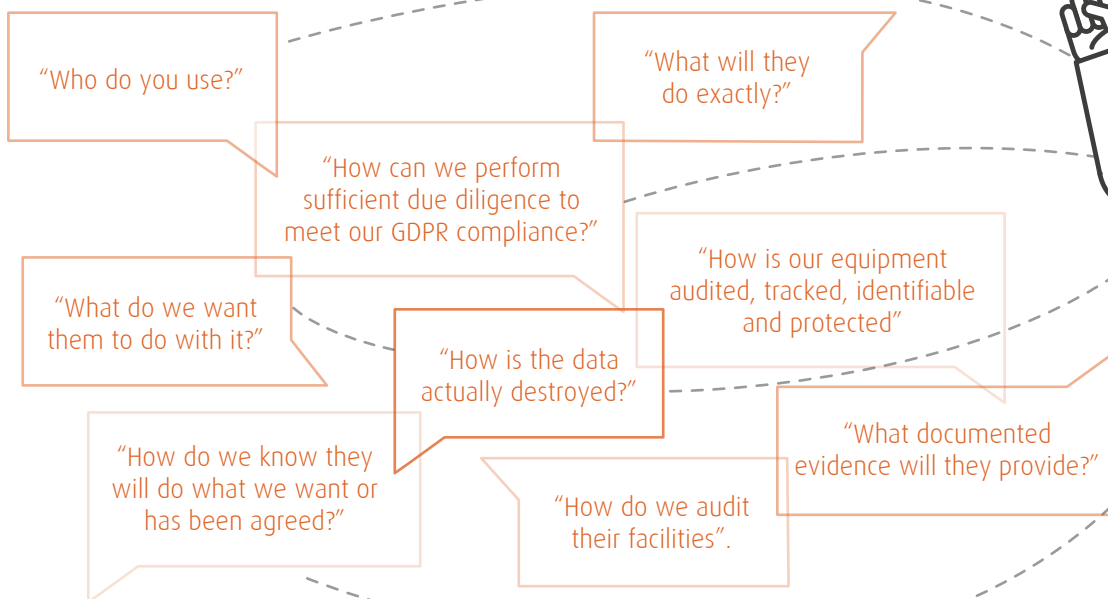
Core risks:

- Personal data on redundant IT equipment.
- Configuration data on equipment that might give someone access to any personal data.
- IP or other sensitive company, client, supplier or staff data.

PROVE you've "done enough to protect"!

IT asset disposal from Blackmore Ricotech evidences you've done enough to protect. You're a data controller, and our work supports your own DPIA (Data Protection Impact Assessment). We answer the questions that the ICO is interested in.

"Who do you use?"

"What will they do exactly?"

"How can we perform sufficient due diligence to meet our GDPR compliance?"

"How is our equipment audited, tracked, identifiable and protected"

"What do we want them to do with it?"

"How is the data actually destroyed?"

"What documented evidence will they provide?"

"How do we know they will do what we want or has been agreed?"

"How do we audit their facilities".

Blackmore Ricotech can provide the 'sufficient guarantees', 'expert knowledge', 'sufficient resources' and can demonstrate the necessary 'technical and organisational measures' required by GDPR, to give your organisation compliance peace of mind.
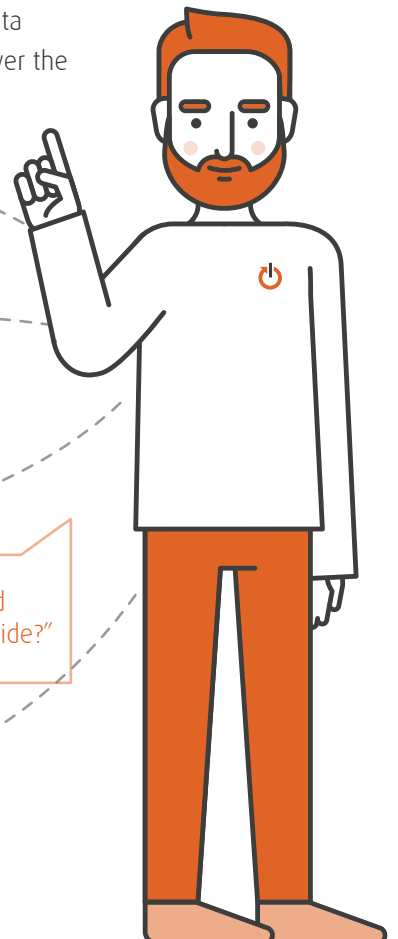
Why use Blackmore Ricotech?

Accreditations

From the outset you'll know that we meet all accreditation requirements from GDPR – including 'expert knowledge' and 'sufficient guarantees'. See page 4.

Contract

We issue a GDPR compliant contract detailing our and your responsibilities and obligations in relation to GDPR and data protection.

Statement of works

We issue a statement of works that details the 'nitty gritty' of the disposal, including contact and site information, list of equipment requiring disposal and details of the equipment disposal processes we have agreed with you.

Range of data assets

Data can be on much more than your computers, laptops, hard drives, networking equipment and phones. We deal with everything.

PCs, laptops, network, printers, mobile phones, memory sticks, CDs, back up tapes, HDDs, IP phones, monitors, peripherals... and much more.

> **We offer a truly end-to-end IT asset disposal service. No stone is left unturned, and nothing is left to chance.**

Richard Connock, Director

On-site audit

Identify and secure data assets to be disposed of. We efficiently ID and record what each item is, if it is potentially data holding or not. An asset number and/or serial number then allocate it a unique 10 digit barcode ID. Allocate each item a container with coded tamper seal where necessary. See our On-site audit factsheet.

Pre-disposal report

Our collection team produces a report which the customer signs on site. Everyone knows exactly what has been removed from site for GDPR compliance.

Security

We use security vetted staff and GPS tracked vehicles and have the technical organisational management measures in place to negate risks from your impact assessments. We transport equipment to our secure facility, without overnight or unscheduled stops, with policies for recognised or unplanned stops. We unload inside our facility under CCTV.

Full tracking

Our barcode tracks every parent or child item (where relevant) from your building to disposal – for our client's peace of mind and compliance. We audit every item before sanitisation, with Government NCSC approved data wiping tools or physical shredding. We provide a full WEEE/audit report and data destruction compliance report within 20 days of every collection

We may find items you have missed, and have a compliant process in place to report on and dispose of these as required. e.g. discs in drives, Flash drives.

Accreditations
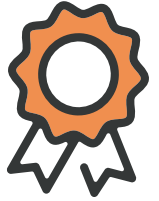
Our accreditations provide evidence that we are experts under GDPR for secure IT asset disposal.

ADISA accreditation

ADISA is recognised by the NCSC (National Cyber Security Centre) and DIPCOG (The Defence INFOSEC Product Co-Operation Group) which is a UK Ministry of Defence forum run by a committee comprised of representatives from the MoD, NCSC and DIPCOG itself. The ADISA auditing process not only confirms verification that we meet the industry-leading IT asset disposal standard, but also includes unannounced spot-check audits. This measures continual conformance to the standard. They provide a FREE monitoring service that enables data controllers to receive copies of audit documents in a timely fashion.

Blackmore Ricotech has ADISA's highest accreditation level – Distinction with Honours.

ADISA has an online academy which also gives members a clear training path for their technical and operational staff to ensure they constantly have the knowledge they need to be effective.

Our other areas of GDPR compliance include:
- adherence to an approved Code of Conduct (since July 2016)
- having contracts in place with our customers OR be able to show where their customers have refused this and, therefore, where the member identifies themselves as not accepting data processing responsibilities.
- meeting the ADISA Standard of risk assessment of the entire process from point of collection to point of data-safe.
- carrying out a data protection impact assessment for data processing operations.

Cyber Essentials

We hold this standard, required when undertaking government contracts to ensure the risks to our own network security have been considered and appropriately secured to prevent Cyber Attacks.

ISO 27001:2013

We hold this internationally recognised Information Security Standard to consider, document and manage the risks involved in the requirements for security techniques of IT assets within an organisation.

Contact us

0800 880 3678 | hello@r3cycle.co.uk | www.r3cycle.co.uk