kefron

FREE GUIDE · IRELAND

Secure IT Disposal Compliance Guide

If you were asked tomorrow,
what could you show?



GDPR, WEEE and data sanitisation explained for Irish organisations retiring IT equipment, with the evidence checklist to keep on file.

Getting rid of old IT is easy. Proving you did it properly is harder.

Most organisations have a process for retiring laptops, servers and phones. Far fewer could hand an auditor, a customer or the Data Protection Commission a clean record of what happened to each device and the data on it.

Under GDPR you are responsible for showing you complied, not just for complying. **This guide is about that evidence.**

What's inside

1. **The rules that apply**
   GDPR, the Data Protection Act 2018 and the Irish WEEE Regulations
2. **Wiping, shredding and the standards behind them**
   Which method suits which media, and which standard to ask for
3. **Your evidence pack**
   The seven records worth keeping for every disposal
4. **The tomorrow test**
   A ten-question checklist to score your current process
5. **Choosing a provider**
   What to ask, and the answers that should worry you

Two sets of rules meet at the end of a device's life

One is about the data on it. The other is about the equipment itself. A compliant disposal has to satisfy both.

The data

GDPR and the Data Protection Act 2018

Article 5(1)(f) · Security
Personal data must be protected against unauthorised access and loss, including on devices you no longer use.

Article 5(2) · Accountability
You must be able to demonstrate compliance. A missing record is treated much like a missing control.

Article 28 · Processors
A disposal provider handling your data is a processor and needs a written contract covering it.

Article 32 · Appropriate measures
Security has to suit the risk, which for data-bearing media means verified erasure or destruction.

The Data Protection Commission is Ireland's supervisory authority. The most serious breaches carry fines of up to €20 million or 4% of worldwide annual turnover, whichever is higher.

The equipment

WEEE Regulations (S.I. No. 149 of 2014)

The European Union (Waste Electrical and Electronic Equipment) Regulations 2014 apply the EU WEEE Directive in Ireland, and the EPA enforces them.

- Business IT equipment can't go into general waste or to an unauthorised collector.
- It has to be reused or treated and recycled through authorised channels.
- Keep the paperwork that shows where it went.

"We wiped it" is not a standard

The right method depends on the media and on whether the device is going to be reused. Whatever is chosen, ask which standard it follows and whether the result was verified.

Reuse possible

Certified software erasure

Overwrites or cryptographically erases the storage, then verifies the result and produces a report for each device. It is the route that keeps equipment fit for refurbishment and resale.

No reuse

Physical shredding

Reduces drives and media to particles, on site or off site. It suits failed drives, media that can't be erased, and data too sensitive to risk. Particle size matters: smaller is needed for SSDs and flash.

Check the standard

What to ask for

NIST SP 800-88 Rev. 2 (September 2025) is the current reference and replaced Rev. 1. **IEEE 2883** covers modern storage. Multi-pass DoD 5220.22-M was written for magnetic drives and isn't a fit for SSDs. Degaussing doesn't work on SSDs either.

! Don't forget the devices outside the server room: phones, tablets, printers and multifunction devices with internal drives, USB sticks, backup tapes and CCTV recorders all hold data.

Seven records to keep for every disposal

If these exist, are complete and match each other, you can answer almost any question about a retired device.

1. **Asset register, reconciled**
   Every device listed by serial number before collection, and checked against what came back.

2. **Chain-of-custody record**
   Signed collection notes showing who took what, when, and every hand-off until processing.

3. **Certificate of Destruction**
   Itemised by serial number, with the method, standard and date for each device.

4. **Erasure reports**
   The software report for each wiped device, showing the erasure was verified.

5. **WEEE recycling records**
   Documentation showing equipment that wasn't reused was treated through authorised channels.

6. **Processor contract**
   The Article 28 agreement with your provider, plus any subcontractors they use.

7. **Provider certifications**
   Current copies of the certificates you relied on when you chose them, with their expiry dates.

Keep them together, per disposal, somewhere you can find them in a hurry. Retain them in line with your records retention policy.

Could you answer yes to all ten?

Pick the last batch of equipment you retired and go through it honestly.

10 yes: you could show it tomorrow.

7–9: close, but fix the gaps before someone finds them.

6 or fewer: it's worth reviewing the whole process.

01	Do you have a list of every device retired, by serial number? ☐
02	Could you match that list to what your provider received? ☐
03	Do you know who handled the equipment at each stage? ☐
04	Was every data-bearing device erased or destroyed, including phones, printers and USB media? ☐
05	Do you know which standard the erasure followed? ☐
06	Do you have an erasure report or certificate for each device, not one for the batch? ☐
07	Is there an Article 28 agreement in place with your provider? ☐
08	Do you hold current copies of your provider's certifications? ☐
09	Can you show where equipment that wasn't reused was recycled? ☐
10	Could you put all of this together within a day? ☐

Questions to ask, and answers to watch for

Ask

- Which sanitisation standard do you follow, and is the software certified?
- Do I get a Certificate of Destruction itemised by serial number?
- How are assets tracked from my building to your facility?
- Are your staff security vetted, and are vehicles tracked?
- Will you sign an Article 28 processing agreement? Who else touches my equipment?
- Which certifications do you hold, and can I see current copies?
- What happens to equipment that can be reused, and do I see the resale value?

Red flags

- One certificate for "50 laptops" with no serial numbers
- "We use DoD 5220.22-M" as the answer for SSDs
- No clear answer on where equipment goes after collection
- Free collection with no paperwork
- Reluctance to sign a processor agreement
- Certifications that are expired, or held by someone else

How Kefron handles it

Kefron's ITAD service in Ireland is built to produce the evidence pack as it goes, from collection to certificate.

1

Secure collection

A trained, security-vetted team collects your assets in GPS-tracked vehicles, with chain of custody from collection to processing.

2

Data destruction

NCSC-certified Blancco erasure, or secure on-site or off-site shredding to 20mm or 6mm particles.

3

Refurbish or recycle

Reusable equipment is refurbished and remarketed. End-of-life assets are recycled in line with WEEE regulations, with a zero landfill guarantee.

4

Certification

A Certificate of Destruction gives you documented proof your data and equipment were securely processed.

Blancco Gold ITAD Partner. NSAI certified to ISO 9001, ISO 14001, ISO/IEC 27001 and I.S. EN ISO 15489-1. Cyber Essentials Plus.

kefron

Want to pass the tomorrow test without the scramble?

Book a consultation with the Kefron ITAD team. We'll go through what you're retiring, the records you need, and how we'd handle it.

Book a consultation



kefron.com

info@kefron.com

Ireland · ITAD services are provided in the Republic of Ireland