DATA SAFE SOLUTIONS

OPERATOR BRIEFING | THE REGULATION COMING DOWN THE TRACKS

New cyber law. And your certificate is in scope.

The Cyber Security and Resilience Bill cleared the Commons in June, was amended in Lords committee in September, and is in its final stages. It pulls relevant managed service providers, data centres and critical suppliers to essential services into direct regulation. Here is what it means for anyone handling end of life data.

FREE TO SHARE

datasafe360.com
September 2026

End of life data has been lightly policed.

For years a process certificate has generally been treated as enough to close the loop on a decommissioned drive. The box left site, the certificate arrived, and the file was closed.

That is about to change, and it changes fastest for the companies who handle other organisations' data and devices.

TREATED AS ENOUGH.

The Cyber Security and Resilience Bill.

Reintroduced after the King's Speech on 13 May 2026, the Bill cleared the Commons on 16 June and was reprinted as amended in Lords committee on 7 September. It is in its final stages.

It brings relevant managed service providers, data centres and critical suppliers to essential services under direct regulation for the first time. For those managed service providers, the regulator is the ICO.

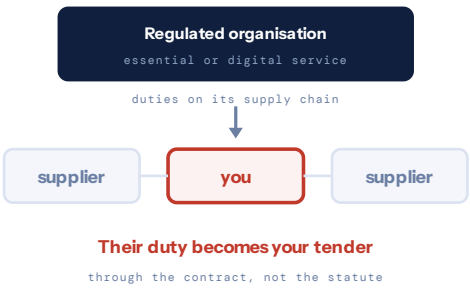
Through the Commons. Amended in the Lords. Final stages.

REAL, CURRENT, NEARLY LAW.

If you serve regulated sectors, you are in the commercial chain.

The Bill does not have to regulate IT asset disposal as a trade to change your market. Regulated organisations are being given stronger duties to manage cyber risk through their supply chains, including through contractual requirements and security checks.

Their obligations become your tender requirements. If you want to keep and win that work, you need the evidence before the tender lands.

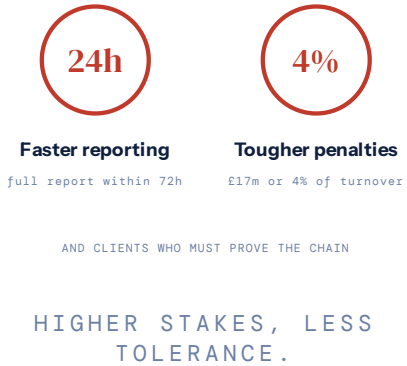


NAMED OR NOT, YOUR MARKET IS CHANGING.

A process certificate will not carry this.

Faster mandatory incident reporting, a light touch notification within 24 hours and a full report within 72. Penalties up to £17 million or 4 per cent of worldwide turnover, whichever is higher. Clients who must prove their supply chain is sound.

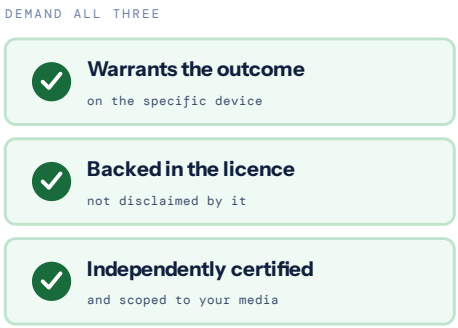
A certificate that says a process ran, with a licence that disclaims the outcome, is exactly what an auditor will pull on.



Evidence, not assurances.

Expect regulated clients to demand device level, warranted, independently certified outcomes they can put in front of their regulator.

The supplier who can hand them that wins the work. The one who cannot becomes the risk they remove.



WHAT YOUR CLIENTS WILL REQUIRE.

We built for this before it arrived.

A warranted outcome on the certificate, backed by uncapped contractual liability and £10 million of professional indemnity insurance. Independently certified to ADISA Product Assurance at Level 5. If the outcome cannot be proven, no successful certificate is issued and no destruction charge is made.

Position now, while it is a differentiator, before it becomes the baseline everyone is held to.

A LIABLE PARTY, NOT A DISCLAIMER.

Do not take our word for it.

Every factual statement in this briefing about the Bill, its progress, incident reporting and penalties comes from Parliament or from the Government's own published factsheets. All of it can be checked without asking us.

THE BILL AND ITS PROGRESS

- **Cyber Security and Resilience (Network and Information Systems) Bill**, Bill 4035, bills.parliament.uk. Source for every date, and for HL Bill 49 as amended in Grand Committee, 7 September 2026.

GOVERNMENT FACTSHEETS PUBLISHED WITH THE BILL

- **Futureproofing.** The commitment to clarify supply chain cyber risk duties, and the statement that they are intended to produce measures such as contractual requirements, security checks and continuity plans. Page 04.
- **Relevant managed service providers.** The definition, and the exclusion of small and micro enterprises. Pages 02 and 04.
- **Designating critical suppliers.** Designation is made by the regulator, not the customer. Page 03.
- **Incident reporting.** Initial notification within 24 hours, full report within 72, the NCSC informed at the same time as the regulator. Page 05.
- **Enforcement.** Maximum penalties of £17 million or 4 per cent of worldwide turnover, whichever is higher, for the more serious tier. Page 05.

REGULATOR MATERIAL

- **Information Commissioner's Office**, published response to the Bill. The ICO as regulator for relevant managed service providers. Page 02.

OUR OWN CLAIMS

- **ADISA Certification**, Product Assurance certificate AAC219, project ADPA039, Assurance Level 5, issued 10 December 2025. Certified product: Data Destruction Engine for Block Storage v2.1. The certificate covers the media types named on it. Ask us for it and read the scope. Page 06.
- **Framework for Conducting a DPIA on End-of-Life Data Destruction**, and its Annex A. Published at datasafe360.com, supplier agnostic, naming no product.