Data Safe Solutions Ltd

FOR ITADS AND DISPOSAL OPERATORS

THE OUTCOME STANDARD

Your clients are about to ask you four questions.

They are being handed those questions in writing, with the evidence behind them. **Today your erasure licence does not let you answer all four with the assurance your client is asking for.** That is not your fault, and it is now a commercial opportunity rather than a problem.

WHAT IS COMING DOWN THE LINE

Four questions you cannot answer yet.

01

How does your software select the correct destruction method for each individual drive?

02

Does your certificate warrant that the data on that specific device is irretrievable, or only that a process completed?

03

When the correct method is refused or unsupported, do you fall back to an overwrite and still certify?

04

What do you pay if data is later recovered from a device you certified?

Read the licence behind whichever product you run. **Every erasure product whose published terms could be examined disclaims the destruction outcome**, excludes liability for loss of data, and caps whatever remains at the fees paid. Not one of them warrants that the data is gone.

That is not a criticism of your supplier. It is the whole market. But it means **your promise to your client cannot exceed the licence underneath it**, and the outcome liability stops with you.

So the honest answer to question four, today, is **nothing.** And your client is about to ask it in writing.

WHY QUESTION ONE DECIDES THE OTHER THREE

The method is chosen by a person, and never checked.

Different media are destroyed by different mechanisms. Get the choice wrong and the tool still reports success, still prints a certificate, and **nobody finds out until someone recovers the data.**

One method does not fit every drive

An overwrite is a reasonable method on a magnetic disk. On flash it is not, because wear levelling, over-provisioning and remapped blocks put physical cells beyond the reach of the host.

The right method there is a firmware level command, or a cryptographic erase on a self encrypting drive. **One method across a mixed batch guarantees some devices get one that cannot work.**

The choice sits with the operator

On conventional platforms the method is determined by a person, either selected at the machine or pre-configured in advance.

Their judgement becomes your evidence, and their mistake becomes your liability.

And it can change without saying so

Where the correct command is refused or unsupported, the common behaviour is to fall back to an overwrite and certify anyway.

The record then names the method that was selected, **not the method that actually ran.**

Selection is the **single point where the outcome is decided**, and nothing checks it afterwards.

THE CHOICE YOU ARE CURRENTLY FORCED TO MAKE

Two kinds of client. You lose something with each.

The ones who insist on destruction

YOU LOSE THE ASSET

241 UK public bodies moved to physical destruction because they could not satisfy themselves software would render data unrecoverable. They accepted the environmental cost and the lost resale value to be certain.

You shred working equipment. **The residual value goes with it, and so does your margin on resale.**

The ones who accept erasure

YOU CARRY THE RISK

437 hold no warranty that the final data state is irrecoverable. 365 named your certificate as their only assurance.

You keep the asset and the resale value. **But the certificate you issue is the weakest link in their evidence chain, and under Article 28 a processor can be held liable and fined in its own right.**

Certainty or value. **Every ITAD is currently choosing one and losing the other.**

WHAT CHANGES

You stop choosing.

The engine interrogates each drive, determines and enforces the correct method itself, and verifies the final data state at the device. **The operator makes no method decision, so the operator cannot get it wrong.** Fallback is not permitted, and the record states whether the data is irretrievable rather than whether a process completed.

To the client who shreds

You can now offer **the certainty they went to physical destruction for, without destroying the asset.**

The equipment comes back into resale. The environmental cost goes away. The assurance is stronger than the one they had, because it is evidenced per device and warranted.

To the client who erases

You can answer all four questions in writing, with clause references.

The certificate stops being the weak link in their evidence chain and becomes the strongest thing in it. **And the outcome liability sits with us, not with you.**

WHAT IT DOES TO YOUR FLOOR

It does not replace your process. It completes it.

Assets are handled, tracked and processed exactly as they are now. Nothing about your chain of custody, your logistics or your grading changes.

Integration

Two way **OpenAPI** connectivity into existing ITAD asset management and ERP systems. Live at NHS Royal Cornwall and across IT Health's Trust estate.

XML output drops into existing erasure software workflows, so it runs alongside what you have rather than replacing it.

DSS Mobile ships ready to deploy and is operational on arrival.

On the floor

The method is selected automatically per device, so **the operator makes no method decision and cannot get it wrong.**

Faster than overwrite, so the same team and the same rigs move more volume, and the trained staff you already have move up into testing, grading and remarketing.

No charge on a failure, and no false pass. A failure is recorded as a failure.

WHAT IT IS WORTH

From process provider to evidence provider.

Win the work

Tenders are beginning to specify outcome evidence rather than a named product. **You can bid for those and answer the specification in full.**

You can also go to the clients who shred and offer them something no process based competitor can.

Keep the asset

Every device that would have been shredded for want of a warranty **comes back into resale instead.**

That is recovered value on equipment you are currently destroying, and a sustainability position you can actually evidence.

Move the risk

The outcome is warranted in our licence and the liability for it is **uncapped and insured.**

You stop standing behind a result your own supplier disclaims.

Offer **the certainty of physical destruction** and **the value recovery of software**. One service, both markets.

WHAT SITS BEHIND IT, AND WHAT TO HOLD ANYONE ELSE TO

Proven. Warranted. Insured.

In the contract

The contractual deliverable is the **Data Destruction Outcome**, achieved only where a Successful Execution Event is recorded.

Irrecoverability is warranted for each successful execution at **clause 5.1**.

Liability for that outcome is **uncapped at clause 17.1**, and is not qualified by a disclaimer elsewhere in the agreement.

Behind the contract

£10 million Technology Professional Indemnity and **£10 million** Public and Products Liability, the professional indemnity on an each and every claim basis.

The **standard inefficacy exclusion is expressly removed by endorsement**, so the cover responds to the destruction itself having failed.

Independently certified to ADISA Product Assurance Level 5. Patent application GB2638704A published.

> These four questions are the ones your clients are being handed, in the companion briefing **Keep your supplier. Mandate the outcome.** Ask us for copies to pass on, and be the supplier who answers them before you are asked.

Put the four questions to your current erasure vendor. Then put the same four to us.

We will answer in writing, so you can compare the two side by side.

hello@datasafe360.com | +44 151 440 3200

2nd Floor, Port of Liverpool Building, Mann Island, Liverpool L3 1BY

datasafe360.com · September 2026