Data Safe Solutions Ltd
EVIDENCE AND STANDARDS PROGRAMME

FREEDOM OF INFORMATION STUDY

The UK Public Sector Data Destruction Gap

The Information Commissioner's Office said a certificate of destruction may be sufficient "as long as you have ensured that the data has been destroyed effectively". That question was put to the UK public sector under the Freedom of Information Act. 437 bodies answered that they had not.

1,036
FOI requests issued to UK public bodies

684
Classified responses in the analysed set

437
Confirmed on the public record that they had not

Second edition, September 2026

FOI requests made by Chris Littlewood as a private individual and published in full at whatdotheyknow.com.
Vendor terms quoted verbatim and dated.

datasafe360.com

The finding

The Information Commissioner's Office was asked whether a certificate of destruction demonstrates compliance. The answer set a condition: a certificate may be sufficient **"as long as you have ensured that the data has been destroyed effectively"**. That question was then put to the UK public sector under the Freedom of Information Act, in requests made by a private individual.

1,036 requests were issued. 684 classified responses came back. **437 organisations confirmed on the public record that they had not.** Every request and reply is published in full at whatdotheyknow.com.

1,036
FOI requests issued to UK public bodies since January 2026

684
Classified responses forming the analysed set

443
Rely on software based destruction

437
Of those, hold no warranty of the outcome

Responses were classified into three models by reference to what each organisation recorded on the public record.

MODEL	BODIES	RECORDED POSITION
1	**6**	Warranted software based destruction. The supplier disclaimer has been contractually overridden.
2	**241**	Physical destruction. Outside the software based assurance question by the organisation's own choice.
3	**437**	Software based destruction with no outcome warranty required or provided, no device specific verification evidence held, and reliance placed on supplier certificates issued under terms that disclaim the outcome.

The FOI question concerned software based erasure. The 241 organisations that moved to physical destruction placed themselves outside it. That leaves 443 bodies relying on software, of which **437 hold no warranty that the final data state is irrecoverable**, and six do.

The pattern holds from HM Treasury, the Cabinet Office and the Environment Agency through NHS Trusts to defence related infrastructure.

These organisations are not failing an invented standard. They are failing the condition the regulator itself attached to the certificate they rely on.

437 is the floor, not the ceiling. The classification credits a pass wherever a response records the medium as physically destroyed, without testing whether a destruction state was evidenced or warranted. Very few of the 241 could evidence either. The true number is higher than 437. This document reports only what the responses prove.

The programme is live and figures are updated as responses arrive. The 1,036 is requests issued, not responses received.

What organisations believe, and what they receive

What organisations believe they are buying

- A guaranteed outcome that data is permanently destroyed
- Proof that the data is irrecoverable
- Liability transferred to the supplier
- Compliance with UK GDPR

What the licence terms actually provide

- Software supplied with the outcome expressly disclaimed
- No warranty of error free or uninterrupted operation
- Liability for loss of data excluded
- Remaining liability capped, commonly at the licence fee

The three sets below are quoted verbatim from the published licence terms of three leading erasure software vendors. Clause references and retrieval dates are given so that any reader can check them.

What the vendor licences say

Blancco Technology Group

End User Licence Agreement · retrieved 9 September 2026

> **CLAUSE 13**
>
> "EXCEPT FOR THE LIMITED WARRANTY SET FORTH ABOVE, THE SOFTWARE IS PROVIDED 'AS IS'."

> **CLAUSE 13**
>
> "BLANCCO DOES NOT WARRANT OR GUARANTEE THAT THE OPERATION OF THE SOFTWARE WILL BE FAIL SAFE, UNINTERRUPTED OR FREE FROM ERRORS OR DEFECTS."

> **CLAUSE 11**
>
> "BLANCCO SHALL NOT BE RESPONSIBLE FOR ANY LOSS OF DATA."

> **CLAUSE 14.2**
>
> Aggregate liability "SHALL NOT EXCEED 100% ... OF THE TOTAL (LICENSE) FEE(S) PAID OR PAYABLE".

Blancco does give a limited warranty above this wording, and it is worth reading closely, because it shows precisely where their warranty stops. It covers the physical medium and substantial conformity with the documentation. It says nothing about the data. Everything past the software behaving as described is disclaimed.
blancco.com/eula/

Certus Software GmbH

Terms and Conditions · retrieved 9 September 2026

> **TERMS AND CONDITIONS**
>
> "The software is provided in the 'as-is state' and Certus Software GmbH does not guarantee or ensure that the operation of the software is secure, uninterrupted or free from any errors or faults."

> **TERMS AND CONDITIONS**
>
> Liability excluded for "lost profits, income or data, business interruption", with any remaining liability that "must not exceed the licensing charges which you have paid".

The entity is Certus Software GmbH, a German company. The first edition of this document named it as a UK limited company in error. certus.software/en/terms-and-conditions/

BitRaser, Stellar Information Technology Pvt. Ltd.

End User Licence Agreement · retrieved 9 September 2026

> **CLAUSE 7**
>
> The software is provided "AS IS" and "AS AVAILABLE", with "NO WARRANTIES OR REPRESENTATIONS of any kind ... or that the Software ... will operate uninterrupted, error-free".

> **CLAUSE 9.1**
>
> No liability for "loss of profits, revenue, business, or data".

> **CLAUSE 9.2**
>
> Liability capped at the fees paid in the twelve months preceding the event giving rise to the claim.

The cap is narrower than a cap on fees paid. A claim arising in year four is measured against year four's fees, not the cost of the licence. bitraser.com/eula.php

These three are illustrative, not exhaustive. Every erasure software vendor whose published terms could be located takes the same position on the destruction outcome. Where a vendor publishes no terms at all, that is recorded as a finding in its own right rather than characterised.

The contradiction

A certificate of destruction and a licence that excludes the outcome cannot both be relied upon.

- If the outcome is guaranteed, liability sits with the party giving the guarantee.
- If liability for the outcome is excluded or capped, no such guarantee exists.

A certificate confirms that **a process was executed**. It does not, on its own, prove that the data is **irrecoverable**.

This is not a defect in any one product. It is what happens when an assurance model built on process documentation is asked to answer a question about outcome.

What UK GDPR requires

The obligations sit across Article 5(1)(f), Article 5(2), Article 24, Article 28(1) and Article 32.

They do not require an organisation to demonstrate that a process was followed. They require it to demonstrate that the measure was **effective**. Article 32(1)(d) makes the point directly, requiring a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures.

In data destruction, effectiveness means one thing: that the final data state is irrecoverable. Where irrecoverability cannot be demonstrated, the data must be treated as still existing and still within scope of UK GDPR, with every obligation that follows.

The regulator's position

The question was put to the Information Commissioner's Office directly. The responses below are from correspondence dated 21 January 2026 under case reference IC-471076-R5B2, quoted in full.

On what makes a certificate sufficient

> "A destruction certificate on it's [sic] own may be a sufficient way to demonstrate compliance, as long as you have ensured that the data has been destroyed effectively. This is likely to depend on the system being used for destruction and how the destruction can be confirmed by the system or the organisation providing the service."

The certificate is not the evidence. It is sufficient only where the controller has already established that destruction was effective, and whether it can be established at all depends on two things the regulator names: **the system used**, and **how the destruction can be confirmed**. That is a description of outcome verification. A certificate that records completion answers neither question.

On certificates carrying disclaimers

> "I can't confirm how the ICO would treat a certificate with the disclaimers you described. Data controllers must do their due diligence and ensure that whoever they use will destroy their data effectively. If the disclaimers don't provide reassurances and confirmations that the data controller needs to confidently say that their data will be destroyed in the way that complies with UK GDPR, they should consider using an organisation that does."
>
> Information Commissioner's Office, correspondence of 21 January 2026, reference IC-471076-R5B2

The regulator will not bless a disclaimed certificate in advance. The duty to establish effectiveness sits with the controller, and where the supplier's terms do not support it, the controller is told to find a supplier whose terms do. That is not a warning about paperwork. It is an instruction about procurement.

The answer to the regulator's condition

The condition was that the controller has ensured the data was destroyed effectively, and that this depends on the system used and on how destruction can be confirmed. Asked what they hold, organisations named the basis of their assurance. It is recorded below exactly as they gave it.

RECORDED BASIS OF ASSURANCE	BODIES
Supplier certificate only. A process certificate from the destruction supplier, with no device level outcome evidence held.	**365**
Process logs only. Logs recording that the process ran, without outcome verification.	**25**
Hybrid evidence. Several artefacts relied on together.	**16**
No recorded assurance at all.	**7**
Standard compliance only. Alignment to a standard, without device level outcome evidence.	**6**
Contractual obligation only. A contractual term, without outcome evidence.	**4**
Explicit outcome warranty. A warrant of irretrievability.	**7**

Physical destruction is recorded under that method and counted separately. Twelve recent responses are not yet assigned a basis.

365

organisations named the supplier's certificate as **their only assurance**

7

hold **a warranty of the outcome**

That is the answer to the regulator's condition, and it is why the question was asked. The Commissioner's office said a certificate may be sufficient as long as the controller has ensured destruction was effective. These organisations named the certificate itself as the thing that satisfies that requirement.

The certificate cannot carry it. As set out earlier in this document, the software that generates those certificates is supplied under licences that disclaim the destruction outcome, exclude liability for loss of data, and cap what remains at the licence fee. The certificate is issued by a vendor who declines, in writing, to warrant the very thing the certificate is being used to prove.

So the assurance runs in a circle. The controller relies on the certificate, the certificate rests on the software, and the software's licence says the outcome is not warranted. Nobody in that chain has accepted responsibility for whether the data is gone, and the only party carrying a legal duty is the one at the start of it.

That is the finding. The regulator set a test and 437 UK public bodies have recorded in writing that they cannot meet it. This is not a failure of intent. It is a failure of the assurance model they were sold, by an industry that excluded the outcome in its contracts while letting the certificate imply it.

The 247 who refused

The most important evidence in this study is not what the 437 do. It is what their peers decided when they looked at the same market.

247 organisations, roughly **36 per cent** of the classified set, have formally positioned themselves **outside software based destruction without warranty**.

Each recorded that position under FOIA, on the public record, under statutory duty. Every one of them has, in effect, **formally rejected the assurance model on which the 437 still rely.**

That is the only thing the 247 have in common, and it is the fact that matters to the 437. Beyond it they did two entirely different things, and the difference between them is the argument of this document.

BODIES	ROUTE TAKEN	WHAT IT COST
241	**Physical destruction.** Certainty bought by destroying the equipment.	Environmental impact, residual asset value, reuse and digital inclusion, higher disposal cost.
6	**Warranted software destruction.** Certainty bought by specifying the outcome in the contract.	Nothing beyond ordinary procurement. The equipment survives.

The 241: a decision, not an accident

These bodies did not arrive at physical destruction through inertia or a lack of technical awareness. Their responses record the opposite. They assessed the software erasure products available to them, they could not satisfy themselves that those products would render data permanently unrecoverable, and a number recorded that assessment and its reasoning in their data protection impact assessments.

That is a documented risk assessment reaching a documented conclusion. A DPIA exists precisely to identify a risk to the rights of data subjects and record what the controller decided to do about it. These controllers identified the risk in software based erasure, wrote it down, and changed method.

They were right about what they read. Every product whose terms could be examined for this study disclaims the destruction outcome. A controller reviewing those licences and concluding that software could not give it confidence was reading the contracts correctly.

What it cost the 241 to be certain

They accepted a price for that certainty, and it is not a small one:

- Environmental impact, from the destruction of functioning equipment
- Loss of residual asset value at the point of disposal
- Reduced reuse and a direct cost to digital inclusion programmes
- Higher direct cost of disposal

Every one of those is a real, quantifiable loss carried by the public purse and by the environment. These organisations paid it anyway, because in their own assessment nothing on the software market justified the alternative. That is how little confidence the assurance model commands among the people who examined it most closely.

The six: the same certainty, without the loss

The other six bodies reached the identical conclusion about disclaimed software, and then did something the 241 did not. Rather than abandoning software destruction, they required the outcome to be warranted, and contracted on that basis. The supplier's disclaimer was overridden by the terms they procured under.

They hold what the 241 went to such lengths for, which is an assurance that the data is gone that does not rest on a certificate the vendor refuses to stand behind. They hold it without destroying a single working machine.

Six is a small number. It is also **proof that the premise the 241 worked from was wrong**: not that software could not be trusted, but that the products they happened to survey could not be.

The route was not exotic. It was ordinary public procurement, specifying an outcome rather than a process, and it is open to any public body that decides to specify it.

What this does to the position of the 437

It removes the three defences that would otherwise be available.

- **That the gap was unknown to the market.** 247 peer bodies identified it and recorded it.
- **That the technical position was unclear.** They reached a clear conclusion on the same evidence.
- **That the alternatives were impractical.** Both alternatives were implemented, one of them at no cost beyond writing a better contract.

Article 5(2) requires a controller not merely to comply but to be able to demonstrate compliance. Where 247 peer public bodies have formally recorded that they discharge that duty by routes the 437 have not taken, the position of the 437 becomes structurally difficult to defend. They have either not looked at the question, or looked and decided not to act, and both of those are recorded positions too.

The two assurance models

Process based assurance

- Certificates
- Logs and erasure reports
- Standards
- Accreditation

Demonstrates that an activity took place. Does not demonstrate the final data state.

Outcome based assurance

- Evidence of the final data state
- Device level verification
- Accountability tied to the result
- Liability extending to the outcome

This is the standard implied by UK GDPR.

Where this leaves ITADs

Article 28(1) requires a controller to use only processors providing sufficient guarantees that processing will meet the requirements of the Regulation. That obligation reaches directly into the IT asset disposal supply chain.

Where certificates are relied on as proof, the underlying software vendor does not warrant the outcome, no device level outcome evidence exists, and the controller believes the outcome is guaranteed, there is an accountability gap on both sides of the contract.

The structural point for any ITAD is that a downstream warranty cannot exceed the upstream one. An ITAD does not control the internal operation of the software it licenses and cannot warrant what that software declines to warrant. A warranty offered on that basis is conditional however it is presented.

The regulator on processor liability

> "Processors can be held liable for non-compliance by relevant investigative and corrective powers of a supervisory authority (such as the ICO) and may be subject to administrative fines or other penalties. However, the ICO works on a case by case basis and I can't confirm what the outcome would be in each case."
>
> Information Commissioner's Office, correspondence of 21 January 2026, reference IC-471076-R5B2

Liability does not stop at the controller. A processor carrying out destruction is exposed to the regulator's investigative and corrective powers in its own right, and to administrative fines. If the final data state cannot be demonstrated, responsibility does not disappear. It remains with the controller and the processor together.

Outcome based destruction, and where DSS sits

The six bodies above did not invent a route. They used ordinary public procurement, and it is open to any public body that decides the outcome is worth specifying.

Data Safe Solutions publishes this study, and states its own position plainly rather than leaving the reader to infer it. What distinguishes the DSS model is not that it is software based. It is that the contractual, evidential and liability positions are aligned to the outcome:

- The primary contractual deliverable is the Data Destruction Outcome
- The outcome is achieved only where a Successful Execution Event is recorded
- Irrecoverability is warranted for each successful execution, at clause 5.1 of the licence
- Liability for that outcome is uncapped, at clause 17.1, and is not qualified by a disclaimer elsewhere in the agreement
- Device level evidential records are produced for each item
- Certificates are evidential records, not process receipts

The outcome also carries bound insurance: **£10 million Technology Professional Indemnity and £10 million Public and Products Liability**, the professional indemnity on an each and every claim basis, with **the standard inefficacy exclusion expressly deleted by endorsement**. That endorsement is the material term rather than the figure, because it is what makes the cover respond to the destruction itself having failed. An insurer does not strike out an inefficacy exclusion for a product it expects to fail.

The licence terms and a specimen certificate carrying an explicit device specific warranty of the final data state are published. Readers are invited to apply exactly the same test to them as this document applies to everyone else, and the insurance schedule is available on request.

EULA: datasafe360.com/wp-content/uploads/2026/04/EULA-DSS.pdf
Specimen certificate: datasafe360.com/wp-content/uploads/2026/01/d4d38a3d-63a1-4f5f-a4e8-034e891ce86e-1.png

Conclusion

The regulator's position is not that certificates are worthless. It is that a certificate counts only where the controller has ensured destruction was effective, and that this turns on the system used and on how destruction can be confirmed.

That condition had never been tested at scale. It has now been tested across the UK public sector, on the public record, and 437 organisations have confirmed that they cannot satisfy it.

Certificates confirm process completion. They do not, on their own, prove irrecoverability. Vendor terms confirm the outcome is not warranted. Organisations believed it was. That gap sits at the centre of accountability under UK GDPR.

247 organisations looked at that gap and stepped outside it. 241 did so by destroying working equipment and absorbing the environmental and financial cost. Six did so by requiring the outcome to be warranted in the contract, and kept their equipment. Both groups reached the same judgement about disclaimed software. Only one of them had to pay for it.

A process can be completed. A certificate can be issued. But if no one is prepared to warrant that the data is irrecoverable, **the risk never left the organisation in the first place.**

Sources and method

The FOI programme, and who ran it. The requests were made by Chris Littlewood **in a personal capacity as a private individual**, not by Data Safe Solutions Ltd. They were submitted through whatdotheyknow.com under his own name, where every request and every response is published in full and permanently. 1,036 requests were issued to UK public bodies under the Freedom of Information Act 2000 from January 2026, and 684 classified responses form the analysed set.

Data Safe Solutions Ltd analyses that public record in this document. It did not make the requests, and it holds no information about any responding body that is not already published. Readers who would rather not take a supplier's word for any of this can read the underlying responses themselves, which is the reason the programme was run in the open. Figures in this document are the cut current at the date of publication; the programme continues and later cuts supersede it.

Vendor licence terms. Quoted verbatim from each vendor's published terms, with clause references, all retrieved 9 September 2026. Copies as retrieved are held on file. Where wording is capitalised in the original it is reproduced as published.

Regulator correspondence. Information Commissioner's Office, case reference IC-471076-R5B2, correspondence dated 21 January 2026 and 28 January 2026, quoted verbatim.

Data Safe Solutions Ltd, 2nd Floor, Port of Liverpool Building, Mann Island, Liverpool L3 1BY. Telephone 0151 440 3200.
hello@datasafe360.com. Company registration 12245066. VAT registration 425206721.
Named vendors are identified by reference to their own published terms, quoted verbatim. Publishing terms that disclaim an outcome is lawful. The finding is the gap between those terms and what purchasers believe they are buying.

WHAT TO DO NEXT

Put these four questions to whoever destroys your data.

Then ask for the answers **in writing**. A supplier who can answer all four on paper is giving you outcome evidence. A supplier who cannot is giving you a process receipt.

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

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

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

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

Then put the same four questions to us.

Ask and we will answer all four in writing, with the clause references. **You will have two sets of answers to the same test**, and you can set the standard you hold today against an outcome based one.

Data Safe Solutions Ltd

hello@datasafe360.com
0151 440 3200
datasafe360.com

2nd Floor, Port of Liverpool Building
Mann Island, Liverpool L3 1BY
Second edition, September 2026