DATA SAFE
SOLUTIONS

ANNEX A · REFERENCE MATERIAL

Reference Material for a DPIA on End-of-Life Data Destruction

Destruction methodologies, the sector evidence record, specimen certificate analysis and procurement specification language. Accompanies the Framework, version 1.4.

> **Advisory, non-commercial, technology neutral and supplier agnostic.**
>
> This annex names no product and no supplier. It does not form part of the framework itself, and its use is not required for the framework to be applied. It does not constitute legal advice. Any DPIA that follows remains the organisation's own document, conducted by its own Data Protection Officer or equivalent function.

Version 2.3	September 2026	Free to share
DOCUMENT VERSION	ISSUED	NO REGISTRATION, NO GATE

Data Safe Solutions Ltd, 2nd Floor, Port of Liverpool Building, Mann Island, Liverpool L3 1BY.
Registered in England and Wales, company number 12245066. · datasafe360.com

CONTENTS

Annex A: Reference Material

ABOUT **Status, scope and how to use it** 1

Where the division of labour sits 1
What is in it 1
A note on the evidential standard used throughout 1

ANNEX A1 **Destruction methodologies and evidence** 3

A1.1 Purpose 3
A1.2 The eight evidential elements 3
A1.3 The three assurance models and their evidential properties 4
A1.4 Destruction methodologies and the evidence each produces 5

ANNEX A1 CONT. **Adequacy across media types** 7

A1.5 Why the media type decides the answer 7
A1.6 Attempted method against applied method, and the fallback problem 9
A1.7 Mapping methodology to the evidential standard 10
A1.8 Why the framework is durable against new technology and new standards 10

ANNEX A2 **Sector evidence summary** 12

A2.1 What the programme asked, and what it did not 12
A2.2 The headline finding 12
A2.3 The scale and spread of the Model 3 cohort 13
A2.4 The cryptographic pattern 14
A2.5 Two responses from bodies with regulatory functions 14
A2.6 What the corpus does and does not establish 15

ANNEX A3 **Comparator analysis of records** 16

A3.1 Purpose and method 16
A3.2 Specimen 1: a process-based certificate (Model 3) 16
A3.3 Specimen 2: a physical destruction record (Model 2) 16
A3.4 Specimen 3: an evidence-based outcome certificate (Model 1) 17
A3.5 Specimen 4: a key reference deletion record 17
A3.6 Comparison against the eight evidential elements 18
A3.7 The reconciliation test illustrated 19
A3.8 How a DPO should read a destruction record 19

ANNEX A4 **Procurement specification language** 21

A4.1 Purpose and how to use this language 21
A4.2 Pathway 1 specification: evidence-based outcome assurance 21
A4.3 Pathway 2 specification: physical destruction with chain of custody 22
A4.4 Cross-cutting specification applicable to both pathways 23
A4.5 Evaluation criteria language 24

REFERENCES **Sources and primary references** 26

ABOUT THIS ANNEX

Status, scope and how to use it

This reference material accompanies the Framework for Conducting a Data Protection Impact Assessment on End-of-Life Data Destruction, version 1.4. It may be drawn upon in conducting such a DPIA. It does not form part of the framework itself, and its use is not required for the framework to be applied.

It is provided as an advisory resource. It is technology neutral and supplier agnostic. It does not constitute legal advice and does not recommend any product, supplier or method. Controllers should satisfy themselves that any DPIA conducted using the framework and this material meets the requirements of their own legal and regulatory advisors and the expectations of the Information Commissioner.

Where the division of labour sits

The framework states the obligation and the method of assessment. This annex carries the technology-specific content. That division is deliberate. New media types and new standards change which methods can produce which evidence, and those changes are made here. The framework's logic does not change with them.

Section references in the form “framework Section 3.2” are to the framework. References in the form A1.5 are to this annex.

What is in it

Annex A1 is the technical reference. It describes the destruction methodologies in current use, the evidence each produces, and whether each is capable of rendering data irretrievable on a given media type. A DPO uses it to answer framework Section 3.2 elements 3 and 4.

Annex A2 is the sector evidence summary. It places a controller’s own position against the recorded practice of 684 UK public bodies, within the scope limits of the programme that produced it. A DPO uses it for context, not for a finding.

Annex A3 is the comparator analysis. It examines four specimen destruction records against the eight evidential elements and sets out a sequence for reading a certificate. A DPO uses it for the mapping at framework Section 3.4.

Annex A4 is sample procurement specification language for each of the two valid mitigation pathways. A DPO passes it to the procurement function once the pathway at framework Section 4.7 is selected.

A note on the evidential standard used throughout

This annex applies the same standard as the framework, and applies it to every method equally. In respect of any specific storage medium, the controller either holds the evidence and the warrant that the data on that medium has been rendered irretrievable, or it does not. Physical destruction is held to that standard on the same terms as software erasure. Neither is given a lighter burden because of what it is.

On any storage device, personal data is either permanently irretrievable or it is not. If data can be recovered using state-of-the-art laboratory techniques, destruction has failed.

ANNEX A1

Technical reference on destruction methodologies and evidence requirements

A1.1 Purpose

This annex sets out the technical material a Data Protection Officer needs in order to apply the assessment criteria at framework Section 3. It explains the destruction methodologies in current use, the evidence each methodology produces, and whether each methodology is capable, on the technical evidence, of rendering data irretrievable on a given media type. It is written to be read alongside the eight evidential elements at framework Section 3.2 and the three assurance models at framework Section 3.3.

The annex is method neutral. It describes the evidential properties of each methodology without recommending one over another. The choice between valid pathways is a matter for the controller under framework Section 4.7. What the annex does establish is that some methodologies are not capable of delivering the outcome on certain media types, and that a DPO must be able to tell the difference.

A1.2 The eight evidential elements

Framework Section 3.2 sets the evidential standard for discharge of the accountability obligation in respect of any specific storage medium. The standard is met only where the controller holds evidence on each of eight elements. They are restated here because the remainder of this annex is organised around them.

1. **Identification of the specific medium.** Evidence that uniquely identifies the storage medium by manufacturer, model, serial number, capacity, interface and media type, and distinguishes it from all other media subject to the same process.
2. **Identification of the destruction method applied.** Evidence recording the specific method applied to the specific medium, with the parameters of the method.
3. **Evidence that the method was appropriate to the medium.** Evidence that the method applied is, on the technical evidence, capable of rendering data irretrievable on that media type.
4. **Verification of the destruction outcome.** Evidence that the method, having been applied, achieved the intended outcome on the specific medium.
5. **Chain of custody before and after destruction.** Evidence that the medium remained in controlled custody throughout.
6. **Date and time of destruction.** Evidence sufficient to correlate with the controller's asset records and the supplier's process records.
7. **Identification of the party effecting destruction.** Evidence sufficient to enable accountability tracing.
8. **An explicit warrant of irretrievability, supplied by the party with control of the destruction process, surviving reconciliation against any governing licence terms or service contract.** The statement that the data on the specific medium has been rendered irretrievable, with responsibility for that outcome accepted by the party making it.

ELEMENT 8 CARRIES THE STRUCTURAL TEST

A record that asserts a successful outcome while the governing licence terms or service contract disclaim responsibility for that outcome is not a warrant. On reconciliation, the disclaimer prevails. This applies to physical destruction service contracts on the same terms as to software licences.

A disclaimer and a liability cap are not the same thing, and this annex does not treat them as such. A term that removes responsibility for the destruction outcome defeats element 8. A financial limit on the liability that flows from that responsibility does not, by itself, negate the warrant. A supplier that states the data on a specific medium has been rendered irretrievable, accepts responsibility if it has not, and caps the resulting financial remedy at a stated sum, has still given a warrant. Whether that cap is commercially adequate is a separate question for the controller's own risk management and procurement judgement. It is not part of the evidential standard.

The technical sections that follow determine which elements a given methodology can produce. Element 8 is contractual, and is examined separately at A3.7.

A1.3 The three assurance models and their evidential properties

Framework Section 3.3 characterises current UK practice at three assurance models. The table summarises the evidential property of each against the eight elements. It is the anchor for the rest of this annex and for the comparator analysis at A3.

MODEL	WHAT IT IS	EVIDENTIAL PROPERTY AGAINST THE EIGHT ELEMENTS
Model 1 Evidence-based outcome assurance	Device-level record of the method applied and the outcome verified, with an explicit warrant of irretrievability from the party with control.	Capable of meeting all eight elements, including the warrant at element 8 surviving reconciliation. Discharges the obligations at Articles 5(2), 24, 28 and 32(1)(d) for the specific medium.
Model 2 Physical destruction with chain of custody	The storage medium is physically destroyed to a destruction state appropriate to the media type, with documented destruction event and chain of custody.	Meets elements 1, 2, 3, 5, 6 and 7 by direct documentation where the record identifies the specific medium. Element 4 is met where the record states the destruction state actually achieved and that state is appropriate to the media type. Element 8 is met where the operator of the destruction process states that the specific medium was reduced to that state and accepts responsibility, in terms that survive reconciliation against the service contract.
Model 3 Process-based assurance	A record states that a process was followed, without recording the elements at framework Section 3.2 for the specific medium and without a warrant that survives reconciliation.	Records that a process ran. Does not, by its contents, evidence that the data on each specific medium has been rendered irretrievable, and does not carry the warrant at element 8. Does not discharge the obligation in its current form.

Model numbering follows the framework. Where other material uses a different numbering, the framework numbering governs. Note that Model 2 is not exempt from elements 4 and 8. A destruction record that states only that equipment was destroyed, without the

state achieved, does not meet element 4, and a service contract that disclaims the destruction outcome defeats element 8 on a Model 2 arrangement exactly as a software licence does on a Model 3 arrangement.

A1.4 Destruction methodologies and the evidence each produces

This section describes the methodologies in current use and the evidence each is capable of producing. The descriptions are technical and neutral. Whether a methodology is appropriate to a given media type is addressed at A1.5.

Overwrite, logical and host-issued

An overwrite operation writes patterns to the host-addressable logical block addresses of the medium, on the principle that the new data replaces the old. Overwrite produces a process record of the passes attempted and the logical capacity addressed. It can support elements 1, 2, 5, 6 and 7. Its capacity to support elements 3 and 4 depends entirely on the media type, because a host-issued overwrite addresses only the space the device controller exposes to the host. On media where the controller retains data outside the host-addressable space, overwrite does not reach that data and cannot evidence that it has been destroyed.

Firmware sanitise commands

Modern storage devices expose internal commands that instruct the device controller to sanitise the medium, including areas not reachable through ordinary host-issued writes. Examples include the ATA Sanitize and Secure Erase commands, the NVMe Format and Sanitize commands, and equivalent commands on eMMC and UFS controllers.

These commands are designed to sanitise data within the media scope defined by the applicable command, including data the host cannot address directly. Whether a particular implementation actually achieved that outcome on a particular device remains a verification question. Command completion alone does not satisfy element 4: a device controller reports what its firmware was written to report, and the framework's objection to process records applies to a device's own success message as much as to a supplier's certificate.

These commands can therefore support element 4 where the device reports completion *and* the result is verified. Two dependencies attach. The command must be supported by the specific device, and it must complete rather than fall back. A1.6 addresses what happens when it does not.

Cryptographic erasure

Where a medium holds all user data in encrypted form, cryptographic erasure destroys the key material itself so that the ciphertext can never be returned to readable form. The ciphertext physically remains on the medium, but the only means by which it could ever be made readable no longer exists. The evidential strength of cryptographic erasure depends on the encryption having been in force over the whole life of the data, on the key material having been generated and held such that it can be destroyed completely, and on the destruction of that key material being verified. Where these conditions hold, cryptographic erasure can support element 4 with verification of key destruction. Where data existed on the medium before encryption was enabled, or where the key management cannot be evidenced, cryptographic erasure does not by itself establish that all historical data is unrecoverable.

Cryptographic scramble

Cryptographic scramble, also termed cryptographic overwrite, rotates and destroys the on-device key at the hardware level, so that the existing ciphertext is permanently orphaned by the device itself. As with cryptographic erasure, the assurance rests on the key material that could unlock the existing data ceasing to exist. Where the device executes the operation and the result is verified, cryptographic scramble can support element 4. The distinguishing feature of both this method and cryptographic erasure is that the key material is destroyed, not merely that a reference to it is removed.

Key reference deletion, which is not a destruction method

Key reference deletion is the deletion of a *reference* to key material, or of a stored or escrowed copy of a key protector such as a recovery key held in a directory service or a cloud tenant, usually accompanied by a logged record that the deletion action occurred. It is not cryptographic erasure and is not a destruction method, and a DPIA should treat it as distinct.

The line between the two is what was destroyed. Where the key material itself is verifiably destroyed, the method is cryptographic erasure or cryptographic scramble and is assessed as such. Where what was deleted is a reference to that material, or one stored copy of a protector for it, the action is administrative and the key material may well survive.

Deleting a stored copy of a key protector removes one means of access. It does not destroy the key material, it does not by itself reach other key protectors that may persist on the device, and the deleted copy may itself have been backed up before deletion. The ciphertext remains intact and potentially recoverable through a surviving protector. A logged record that a deletion was performed is evidence that an administrative action occurred, which is process, not evidence that the data has been rendered irretrievable, which is outcome. This is the same process against outcome gap described elsewhere in this annex, relocated to the key.

Encryption is a control for the protection of data at rest during the operational life of the device. The deletion of a key reference does not convert that at-rest control into a method that discharges the end-of-life obligation. Cryptographic erasure and cryptographic scramble destroy the key material; key reference deletion does not, and on that distinction the adequacy of the method turns.

Physical destruction

Physical destruction renders the medium physically inoperable by shredding, crushing, disintegration or, for magnetic media, degaussing. The medium ceases to exist as a functioning device. Physical destruction supports elements 1, 2, 5, 6 and 7 by direct documentation where the record identifies the specific medium. It supports element 4 where the record states the destruction state achieved and that state is appropriate to the media type. The qualification at A1.5 is material: a particle size adequate for one media type may leave data recoverable on another.

Operations that are not destruction methodologies

Removing the file system structure of a medium by partitioning, formatting or factory reset does not, in general, overwrite the underlying data. Such operations leave the data recoverable using standard forensic tools. They produce a record that an operation occurred but cannot support element 4 on any media type, and do not discharge the Article 5(2) obligation in any context. A DPIA should treat a record that shows only a format, partition or reset as recording that no destruction methodology was applied.

ANNEX A1 CONTINUED

Methodological adequacy across media types

A1.5 Why the media type decides the answer

The central technical question for a DPIA is whether the method applied to a specific medium is capable of rendering the data on that media type irretrievable. The answer differs by media type, and the difference is the principal source of methodological risk in the sector.

Magnetic media: rotating hard disk drives

On rotating magnetic media, a single-pass host-issued overwrite of the host-addressable space has historically been treated as effective, because the logical and physical layouts correspond closely and the host addresses substantially all of the medium. The residual consideration is remapped sectors. A drive that has reallocated sectors during operational life may hold data in reallocated physical sectors that a host-issued overwrite does not reach. Degaussing is effective on magnetic media because it disrupts the magnetic domains across the whole platter. Degaussing is not effective on flash media, which holds data as electrical charge rather than magnetic orientation.

Flash media: SSD, NVMe, eMMC, UFS

Flash media does not present a fixed correspondence between the logical addresses the host sees and the physical cells that hold the data. A Flash Translation Layer in the device controller manages the mapping and changes it continuously. Three behaviours of that layer defeat host-issued overwrite as a destruction method.

1. **Wear levelling.** To spread write wear evenly, the controller writes new data to different physical cells rather than overwriting the cells that held the previous version. A host overwrite of a logical address therefore typically lands on different physical cells, leaving the original data resident and recoverable from the cells that previously held it.
2. **Over-provisioning.** Flash devices reserve physical capacity beyond the advertised host-addressable capacity, commonly a substantial proportion of the device. Data migrates into the over-provisioned area during normal operation. A host overwrite cannot address the over-provisioned area at all, so any data resident there is not reached.
3. **Bad-block remapping.** Cells that the controller retires as unreliable may still hold readable data, and are no longer addressable by the host, so a host overwrite cannot reach them.

The consequence is that an overwrite-based method applied to flash media may complete and report success while leaving data recoverable in cells the host could not address. This is not a configuration error. It is a structural property of how flash media is managed, and it has been demonstrated experimentally: Wei and others at the University of California, San Diego, tested a range of flash devices and found data recoverable after software overwrite procedures that reported success, precisely because of Flash Translation Layer behaviour.

The methods capable of addressing this on flash media are a firmware sanitise command that operates on the media scope the command defines, completes rather than falling back, and is verified; a cryptographic

erasure or scramble where the conditions at A1.4 hold; or physical destruction to a particle size appropriate to flash. In each case the method has to be verified rather than assumed, for the reasons given at A1.4.

What the standards do and do not settle

Reference points recur in supplier documentation and are commonly relied upon by controllers. A DPO should understand the scope of each.

NIST SP 800-88 Revision 2 supersedes Revision 1 of December 2014. It retains the sanitization programme and the three categories, Clear, Purge and Destroy. Clear is logical sanitisation using host read and write commands. Purge applies media-specific techniques, including firmware commands and cryptographic erasure, that resist laboratory recovery. Destroy is physical destruction. Revision 2 strengthens the treatment of validation and, other than for cryptographic erase, no longer carries its own technique and tool tables. It directs organisations instead to comply with IEEE 2883, NSA specifications, or an organizationally approved standard. A record that shows a Clear-level operation on flash media has, on the face of the standard it cites, not applied a method that standard treats as sufficient to resist recovery on that media type.

IEEE 2883-2022 specifies methods for sanitizing logical and physical storage and provides technology-specific requirements and guidance for the elimination of recorded data. It is the standard NIST now points to for technique-level requirements. **IEEE 2883.1-2025** is the accompanying recommended practice for applying those methods before reuse, resale or disposal.

HMG Information Assurance Standard No. 5 originated as an overwrite-based standard developed for magnetic media. It predates the dominance of flash storage and was conceived against the physical characteristics of magnetic media. It has been superseded by NCSC guidance on the secure sanitisation and disposal of storage media. A controller relying on an overwrite specification derived from a magnetic-era standard, applied to a flash estate, is relying on a method whose adequacy on the actual media type is not established by the standard it cites.

> **THE PRINCIPLE TO CARRY FORWARD**
>
> Citation of a recognised standard is not, by itself, evidence that the method applied was appropriate to the specific media type. The standard must be read for what it actually addresses, and the level applied within the standard must be the level appropriate to the media.

Devices where storage and key management are integrated and not host-verifiable

A distinct adequacy question arises for device classes in which the storage medium and its sanitisation are managed entirely by an integrated controller or a hardware key subsystem, with no host-accessible path by which the outcome can be independently verified. This characteristic is present in current mobile devices, in tablets, and in laptops and other devices built on integrated systems-on-chip where the storage is soldered and controller-managed and a hardware key subsystem holds the media encryption key. The point is the technical characteristic, not the manufacturer or product line: the assessment applies to any device with this architecture, and does not apply to a device of the same outward type that exposes a removable, host-addressable storage medium.

On such a device, a sanitisation operation typically instructs the controller or the key subsystem to destroy the media key and then reports completion. That report is an assertion by the device that the operation succeeded. It is not independently verifiable outcome evidence, because no party outside the integrated subsystem is in a position to confirm that the key material has in fact been destroyed and that no recoverable path to the data remains. This is the same structure described elsewhere in this annex, an action asserted without verifiable evidence of the outcome, and it engages elements 4 and 8 in the same way.

The technical literature and standards reviewed for this annex, listed in the references, have not identified a generally available software-based method for these device classes that produces independently verifiable outcome evidence capable of being warranted to the standard at framework Section 3.2. This is a statement about what the reviewed sources establish. It is not a claim of knowledge about every proprietary device architecture in existence, and a controller presented with such a method should assess it on its merits rather than treat this paragraph as excluding it.

On that basis, a DPIA assessing these devices should expect that Pathway 1 will not be available for them on the methods currently in general use, and that the assessment routes to Pathway 2, physical destruction to a particle size appropriate to the media, as the route by which the obligation is discharged. That Pathway 2 arrangement must itself meet the requirements at framework Section 4.3, including the recorded destruction state and the warrant surviving reconciliation.

Three things would change this conclusion for a given device class, and a DPIA should look for all three together: a method that operates on the full media scope; outcome evidence that a party outside the integrated subsystem can verify rather than a completion message from the device itself; and a party with control of that method willing to warrant the outcome on the specific medium. Where those exist, the assessment routes the method through Pathway 1 in the ordinary way. The framework's logic is unchanged; what changes is whether a method meeting the standard exists.

A1.6 Attempted method against applied method, and the fallback problem

A material distinction for a DPIA is between the method a process attempted and the method it actually applied. A destruction process may attempt a higher-assurance firmware command and, where the command is unsupported by the device firmware or fails on the device, fall back to a lower-assurance overwrite, then complete and report success. The record may show both events, with the higher-assurance method shown as failed and the lower-assurance method shown as completed.

The risk for a controller is twofold. First, a record that reports an overall pass may conceal that the method actually applied was the lower-assurance fallback, which on flash media may not have achieved the outcome. Second, where the record reports the fallback transparently, the controller still needs to read it accurately and assess the applied method, not the attempted method, against the standard at A1.5.

A DPIA should establish whether the controller is in a position to read its records at this level of detail, and should treat the applied method, not the attempted method, as the basis for the element 3 and element 4 assessment.

A1.7 Mapping methodology to the evidential standard

The table maps each methodology to the evidential elements it is capable of supporting, by media type. It records capability, not whether any given supplier's record actually contains the evidence. A methodology that is capable of supporting an element still produces the element only where the record and supporting documentation contain it.

METHODOLOGY	MEDIA TYPE	CAN SUPPORT ELEMENT 3, METHOD APPROPRIATE?	CAN SUPPORT ELEMENT 4, OUTCOME VERIFIED?
Host-issued overwrite	Magnetic (HDD)	Yes, subject to remapped sectors	Where read-back verified and remapped sectors addressed
Host-issued overwrite	Flash (SSD, NVMe, eMMC, UFS)	No. Does not reach over-provisioned or remapped cells	No. Host verification cannot confirm cells the host cannot address
Firmware sanitise command, completed	Flash and magnetic	Yes, where supported and not fallen back	Yes, where the device reports completion and the result is verified
Cryptographic erasure or scramble, key material destroyed	Self-encrypting media	Yes, where the A1.4 conditions hold	Where key-material destruction is verified and encryption was in force throughout
Key reference deletion, key material not destroyed	Any	No. Not a destruction method	No. Ciphertext intact and surviving protectors may persist
Device-asserted erase on integrated, non-host-verifiable devices	Mobile, tablet, integrated-SoC laptop with soldered controller-managed storage	Device-dependent, not independently verifiable	No established method produces verifiable, warrantable outcome evidence (see A1.5)
Physical destruction	Any, to a media-appropriate destruction state	Yes, where the state achieved suits the media	Where the state achieved is recorded and suits the media
Partition, format or reset	Any	No. Not a destruction method	No

A1.8 Why the framework is durable against new technology and new standards

The framework is constructed so that it does not need revision each time a media type, a methodology or a standard changes. Three design choices give it that durability, and a DPO should rely on them rather than on any list of current technologies.

1. **The obligation is anchored to the outcome, not the method.** The standard at framework Section 3.2 asks whether the data on the specific medium has been rendered irretrievable, with a warrant from the party with control. That question is media neutral and method neutral. A new media type or a new methodology enters the assessment as a new instance of the same question, not as a gap in the framework.

2. **The assessment criteria evaluate evidence, not technology.** Framework Section 3 evaluates the evidence the controller holds against the eight elements. New technology changes which methods can produce elements 3 and 4, which is addressed by updating this annex rather than the framework.

3. **The forward-compliance risks are stated by direction, not by instrument.** Framework Section 2.6 frames the regulatory direction as a movement towards outcome-evidence-based accountability. The Cyber Security and Resilience (Network and Information Systems) Bill, introduced in the House of Commons in November 2025 and in Lords committee stage at the date of this annex, extends the perimeter to relevant managed service providers and provides for the designation of critical suppliers. It does not name the end-of-life IT disposal chain as a regulated category. What it evidences is closer scrutiny of technology supply chains, and a controller that holds a warrant of irretrievability for each specific medium is positioned for that direction whatever the final form of the instrument.

The practical implication is that this annex carries the technology-specific content and is the document to revise as media types and standards evolve. The framework states the obligation and the method of assessment, and remains stable.

ANNEX A2

Sector evidence summary on current destruction assurance practice

A2.1 What the programme asked, and what it did not

This annex summarises what a Freedom of Information programme conducted across the UK public sector establishes about current destruction assurance practice. The purpose is to place a controller's own position in context. It is not a comment on any individual body.

The scope of the programme determines what the evidence can and cannot support, so it is stated first. Each request asked two questions:

1. whether the body's policies, contractual terms or internal procedures require an explicit outcome-based warranty that personal data on a specific storage device has been rendered irrecoverable following **software-based erasure**; and
2. what recorded evidential assurance is relied upon to conclude that the final data state is irretrievable.

> THE SCOPE LIMIT, AND WHAT FOLLOWS FROM IT
>
> The requests **expressly excluded physical destruction methods** from the scope of the software-based assurance question. The programme therefore did not assess, and this annex does not report, whether any body's physical destruction practice satisfies the evidential standard at framework Section 3.2.
>
> Nothing in this section should be read as evidence that physical destruction as practised in the UK public sector meets that standard, or that it does not. The requirements a physical destruction arrangement would have to satisfy are set out at A1.4, A3.3 and A4.3, and they are as demanding as those applied to software erasure.

Bodies were asked to answer by reference to recorded information held. Responses are on the public record and individually retrievable through the WhatDoTheyKnow platform.

1,036 requests were issued across the programme. 684 have produced classified responses, which form the analysed set. The remainder are awaiting response, or were returned as department-dependent, refused, or not held, and are not counted. The programme is live; figures are stated as at the date on the cover.

A2.2 The headline finding

The 684 classified responses fall into three groups. The categorisation is taken from the bodies' own answers, given under statutory duty under the Freedom of Information Act 2000, rather than from analytical inference.

RECORDED POSITION	BODIES	WHAT THE BODY STATED
Software-based erasure with an explicit outcome warranty	6	Policies, contractual terms or supplier arrangements require an explicit outcome-based warranty that personal data on a specific storage device has been rendered irrecoverable.
Physical destruction	241	Reliance on physical destruction methods for end-of-life data-bearing equipment. These bodies placed themselves outside the scope of the software-based assurance question by their own answer.
Software-based erasure without an outcome warranty	437	No explicit outcome-based warranty is required or provided; no device-specific documentation evidencing independent verification, testing or validation is held beyond supplier accreditation or process completion; reliance is placed on supplier destruction certificates issued under terms that disclaim outcome warranty.
Total classified responses	**684**	

The 241 bodies in the middle row are not reported here as compliant, and the programme did not test them. They are reported because their answers establish the denominator for the question that was asked.

443 bodies to which the software assurance question applied	**437** hold no outcome warranty	**6** require an explicit outcome warranty

Of the bodies that use software-based erasure and were therefore asked the question, six hold an explicit outcome warranty and 437 do not.

That is the finding. It is not a claim that software erasure fails, and it is not a claim about the adequacy of any product. It is a statement about what the responding bodies record: that in the overwhelming majority of cases the controller holds a supplier certificate issued under terms that decline responsibility for the outcome, and holds nothing else at the level of the specific device.

Two consequences follow for a controller conducting a DPIA. The first is that a finding of Model 3 in the controller's own assessment places it with the substantial majority of its peers, which is relevant to the risk assessment at framework Section 2 but does not soften the finding, because the obligation is owed by each controller individually. The second is that warranted software-based destruction is not a hypothetical procurement proposition. Six public bodies have specified and obtained it, so the route exists and is available.

A2.3 The scale and spread of the Model 3 cohort

The 437 bodies recording software-based erasure without an outcome warranty are not concentrated in one part of the public sector. The cohort runs through central government departments and their agencies, the criminal justice system, the NHS at trust and integrated care board level, the devolved administrations of all three nations, regulators, and the majority of responding local authorities.

The significance for a DPIA is that the gap is architectural rather than local. A controller that finds its own arrangements at Model 3 has found a property of the assurance architecture it bought into, not a failure of

diligence peculiar to itself. That does not discharge the obligation, but it does tell the DPO what kind of problem is being assessed, and it indicates that the remedy lies in specification and contract rather than in supplier performance management.

A2.4 The cryptographic pattern

A distinct pattern within the Model 3 cohort is of particular relevance to the methodological distinction at A1.4. A number of bodies recorded reliance on a cryptographic method, described in their responses as encryption with deletion of the encryption key, as the basis on which they conclude that personal data at end of life has been rendered irretrievable.

This is not a variant of the supplier certificate position. It is a distinct pattern and, on the framework's reasoning, a weaker evidential position rather than a stronger one. A body relying on a supplier certificate at least believes the data has been destroyed. A body relying on key reference deletion has data that, on its own account, physically remains on the medium in encrypted form, and asserts that the means of reading it has been removed, on the strength of a logged record that a deletion action occurred.

The pattern is illustrated by a response from a Scottish Government body, made under the Freedom of Information (Scotland) Act 2002, which stated its evidential assurance for end-of-life devices to be the deletion of the device's recovery key in its directory service and cloud tenant, with that deletion logged. Read against the eight elements, the response evidences that an administrative action was performed and logged, which addresses elements 6 and 7, while the elements that evidence the outcome, elements 3, 4 and 8, are not addressed. It does not evidence that the key material itself was destroyed, that no other key protector or backup of the deleted key survives, or that the whole medium was encrypted from first use with no unencrypted data resident.

The body grounded its position in compliance with the applicable government secure sanitisation requirements, so the response also illustrates the wider pattern in this annex: that citation of a recognised standard, and performance of the action it describes, does not by itself produce evidence of the outcome. Compliance with government secure sanitisation guidance and the controller's accountability obligation under UK GDPR are independent regimes, and satisfying the first does not satisfy the second.

The significance for the wider evidential picture is that the accountability gap is not an artefact of one assurance route. It reappears independently among bodies that adopted what they understood to be a more modern alternative to a supplier certificate. This example is anonymised.

A2.5 Two responses from bodies with regulatory functions

Two responses from public bodies that are themselves environmental regulators are particularly useful as evidence of sector practice. Neither is the data protection regulator, and neither response is relied upon here as an authoritative interpretation of Article 5(2). They are relied upon only as formal accounts, given under statutory duty and on the public record, of those bodies' own assurance arrangements.

The **Scottish Environment Protection Agency**, in its formal response of 31 March 2026, characterised its own position as "a gap in our Data Protection Accountability obligations for this processing", and identified the remedy as the drafting of a Data Protection Impact Assessment for the specific processing. The characterisation as a gap is the Agency's own, and the remedy it identified is the one this framework sets out.

The **Environment Agency**, across a sequence of responses between February and May 2026, narrowed its position to the statement that its destruction certificates do not provide a guarantee that personal data has been rendered irrecoverable. The Agency is the English government body with environmental regulation responsibility for IT disposal and is itself under the jurisdiction of the Information Commissioner.

These accounts are not used here to criticise the bodies concerned. Their value is that the characterisation of the gap is the bodies' own rather than an external assertion, and that both sit within the 437.

A2.6 What the corpus does and does not establish

For a controller conducting a DPIA, the sector evidence supports the following, and only the following.

What it establishes

1. **Software-based erasure without an outcome warranty is the prevailing arrangement.** Of the 443 bodies asked, 437 hold no outcome warranty. A controller finding the same in its own assessment is in the substantial majority.
2. **The warranted alternative exists in the market.** Six public bodies have specified and obtained software-based destruction with an explicit outcome warranty. Pathway 1 at framework Section 4.2 is a live procurement route, not a theoretical construct.
3. **The recorded basis most controllers rely on is the supplier certificate.** That directs the DPIA to the reconciliation test at framework Section 3.2 element 8, and to the comparator analysis at A3.

What it does not establish

1. **Nothing about the adequacy of physical destruction.** The 241 bodies recording physical destruction were outside the scope of the assurance question. Whether their arrangements satisfy the eight elements was not asked and is not answered here. A controller using Pathway 2 must assess it against A4.3 on its own terms.
2. **Nothing about whether any individual body is compliant.** The corpus records what bodies said they hold. It does not adjudicate any body's position under UK GDPR.
3. **Nothing that substitutes for the controller's own assessment.** This summary places a controller in context. The finding comes from the controller's own evidence, examined under framework Sections 3.4 and 3.5.

ANNEX A3

Comparator analysis of specimen destruction records

A3.1 Purpose and method

This annex analyses four specimen destruction records, each representative of a pattern found in current practice, against the eight evidential elements at framework Section 3.2. The purpose is to show a DPO what to look for when examining the controller's own records under the mapping exercise at framework Section 3.4.

The specimens are representative composites, not the record of any named supplier. The analysis is supplier agnostic by design: it examines the evidential characteristics that distinguish the models, not the merits of any product. When the DPO applies this analysis, the operational records the controller actually receives are the relevant evidence, and they should be obtained as specimens under framework Section 3.4 and examined against the elements directly.

A3.2 Specimen 1: a process-based certificate (Model 3)

A representative process-based certificate records that a destruction or erasure process was executed. It typically states the date, the operator or supervisor, the method by reference to a named standard, and a result of "pass" or "erased". It may reference the host device, for example a desktop or laptop asset tag, rather than the data-bearing storage medium within it. It is commonly described as a certificate of erasure, a sanitisation report, an audit record or a process attestation.

What it does not record is the specific storage medium by serial number distinct from the host device, the method actually applied to that specific medium as distinct from the standard referenced, evidence that the method was appropriate to the medium's type, outcome verification on the specific medium, or an explicit warrant of irretrievability. Where the governing licence terms or service contract disclaim responsibility for the outcome, exclude liability for data loss, and cap liability to the fee paid, the certificate's apparent assertion of success does not survive reconciliation against those terms.

A3.3 Specimen 2: a physical destruction record (Model 2)

A representative physical destruction record documents that a storage medium was physically destroyed. At its strongest it records the medium by serial number, the destruction method such as shredding to a stated particle size or degaussing to a stated field strength, the date, time, location and operator of the destruction event, and the chain of custody from collection to destruction. It may include photographic or video evidence and a record of the disposition of the destroyed material.

Two things determine whether such a record meets the standard, and neither is supplied by the fact of destruction.

The first is whether the destruction state achieved is *recorded* and is *appropriate to the media type*. A record that states equipment was destroyed, without the particle size or field strength achieved, does not evidence element 4. A record that states a particle size developed for hard disk drives, applied to solid state media, evidences a state that may leave intact memory packages, and so does not evidence element 3.

The second is whether the operator's statement survives reconciliation. Physical destruction service contracts frequently contain the same outcome disclaimers found in destruction software licences, stating that the supplier accepts no responsibility for whether data has in fact been rendered irretrievable. Where they do, element 8 fails on a Model 2 arrangement exactly as it fails on a Model 3 arrangement, and the fact that the medium no longer exists does not repair it. What the controller needs is a statement by the operator that the specific medium was reduced to the recorded state, with responsibility for that statement accepted and not disclaimed. A cap on the financial remedy is a different matter and does not, by itself, defeat the element, as set out at A1.2.

In practice, much of what is presented to controllers as a physical destruction record is weaker than the specimen described here: a collection note, a weight ticket, or a statement that a quantity of equipment was destroyed. None of those identifies a medium, records a state, or carries a warrant.

A3.4 Specimen 3: an evidence-based outcome certificate (Model 1)

A representative evidence-based outcome certificate records the specific medium by manufacturer, model, serial number, capacity, interface and media type; the method actually applied to that medium with its parameters; the basis on which the method is appropriate to the media type; the verification of the outcome on that specific medium, such as read-back verification or verified destruction of the key material; the chain of custody; the date and the party effecting destruction; and an explicit warrant that the data on the specific medium has been rendered irretrievable, with responsibility for that outcome accepted by the party with control of the destruction process.

The governing contractual documents align with rather than disclaim the warrant, so the warrant survives reconciliation. A certificate recording a genuine cryptographic erasure or cryptographic scramble, where the key material itself was verifiably destroyed, sits within this model where it records the elements above for the specific medium.

A3.5 Specimen 4: a key reference deletion record

A representative key reference deletion record states that a reference to key material, or a stored or escrowed copy of a key protector such as a recovery key held in a directory service or cloud tenant, was deleted, and that the deletion action was logged. It typically identifies the host device, the date, and the administrative action performed, and points to an audit log entry as the assurance.

The record is distinct from Specimen 3 and must not be read as a cryptographic erasure certificate. What it records is that an administrative action was performed and logged. What it does not record is that the key material itself was destroyed, that no other key protector or backup copy of the deleted key survives in any directory service, cloud tenant, key management system, escrow or backup, or that the whole medium was encrypted from first use with no unencrypted data resident. The ciphertext remains on the medium.

As A1.4 sets out, deletion of a key reference is not destruction of the key material, and is not a destruction method. A DPIA should place this specimen with the process-based group at Specimen 1 for the purposes of the finding, because what it evidences is process, not outcome, notwithstanding that the underlying technology is encryption rather than overwrite.

A3.6 Comparison against the eight evidential elements

The four specimens map to the eight elements as follows. “Present” means the element is recorded for the specific medium. “General” means it is recorded only at the level of the batch, the host device or the referenced standard. “Absent” means it is not recorded.

EVIDENTIAL ELEMENT	1. PROCESS	2. PHYSICAL	3. EVIDENCE-BASED	4. KEY REFERENCE DELETION
1. Specific medium identified	General, often host device	Present, where the record identifies the medium	Present	General, host device
2. Method applied to that medium	General, standard referenced	Present	Present	Deletion action recorded
3. Method appropriate to media type	Not evidenced	Present only where the state achieved suits the media type	Present	Not evidenced
4. Outcome verified on the medium	Absent	Present only where the destruction state achieved is recorded	Present	Absent, key material not shown destroyed
5. Chain of custody	Variable	Present	Present	Variable
6. Date and time	Present	Present	Present	Present
7. Party effecting destruction	Present	Present	Present	Present
8. Warrant surviving reconciliation	Absent, disclaimed by licence terms	Present only where the operator warrants the state and the service contract does not disclaim it	Present, aligned to contract	Absent, no key-material destruction

The pattern is the point. Specimen 1 records the elements that evidence activity, elements 6 and 7, while the elements that evidence outcome, elements 3, 4 and 8, are absent or recorded only in general terms. Specimen 4 follows the same shape as Specimen 1 despite using encryption rather than overwrite: it records that an action was performed and logged, while the outcome elements are absent.

Specimen 2 is capable of recording the outcome elements but frequently does not. It is the specimen most often assumed to be sufficient without examination, and a DPO should examine it with the same care as Specimen 1 rather than accepting physical destruction as self-explanatory. Specimen 3 records the outcome elements for the specific medium by design.

The distinction the DPIA must draw is between a record of activity and evidence of outcome. It is a distinction about evidence, not about the underlying technology, and not about whether the medium still exists.

A3.7 The reconciliation test illustrated

The reconciliation test at element 8 is the one most often missed, because the record and the governing terms are usually read separately and at different times. The record is read at the point of assurance, by the operational team. The terms are read, if at all, at the point of procurement, by a different function.

Read together, a certificate stating that a drive was successfully erased, set against a licence that supplies the software on an “as is” basis with no warranty of effectiveness and an exclusion of liability for data loss, produces a net position in which no party has accepted responsibility for the outcome. On reconciliation, the disclaimer prevails.

The same test applies to physical destruction. A destruction certificate set against a service contract that excludes liability for the destruction outcome and caps liability at the value of the collection produces the same net position, and the DPIA should record it the same way.

What the test looks for is the presence or absence of accepted responsibility for the outcome, not the size of the remedy attached to it. A supplier that warrants the outcome and limits its financial liability to a stated sum has satisfied element 8; the adequacy of that limit is a procurement and risk question the controller answers separately, and the DPIA should record it as such rather than as an evidential failure. A supplier that declines responsibility for the outcome has not satisfied element 8, whatever the liability position.

A DPIA should require the record and the governing terms to be read together, by a function competent to reconcile them, and should record the net position rather than the record’s assertion taken in isolation.

A3.8 How a DPO should read a destruction record

The following sequence allows a DPO to place any record against the models without specialist tooling.

1. Identify whether the record refers to the storage medium by its own serial number, or only to the host device. If only the host device, element 1 is general, not present.
2. Identify the method actually applied to the specific medium, not the standard referenced. If only a standard is named, element 2 is general.
3. Establish the media type and ask whether the applied method is appropriate to it under A1.5. An overwrite recorded against flash media does not satisfy element 3.
4. Where the record relies on a cryptographic method, establish whether it evidences destruction of the key material itself, or only the deletion of a key or a stored copy of a key protector. A logged deletion of a recovery key is key reference deletion, not cryptographic erasure, and does not satisfy element 4 under A1.4.
5. Where the record is of physical destruction, look for the destruction state actually achieved, and ask whether that state is appropriate to the media type. A statement that equipment was destroyed does not satisfy element 4, and a hard disk particle size applied to solid state media does not satisfy element 3.
6. Look for outcome verification on the specific medium. A result of “pass” that reports process completion is not outcome verification. If absent, element 4 is absent.

7. Obtain the governing licence terms or service contract and reconcile them against the record's assertion. If the terms disclaim the outcome, element 8 is absent however the record is worded. This step applies to physical destruction contracts as well as to software licences.

8. Record the model the record falls into, and carry the finding into the assessment at framework Section 3.5.

ANNEX A4

Sample procurement specification language

A4.1 Purpose and how to use this language

This annex provides sample specification language for the procurement of destruction services under each of the two valid mitigation pathways at framework Section 4. The language is for adaptation by the controller's procurement function, in coordination with the controller's legal advisors. It is supplier agnostic and neutral between the two pathways, and names no product. It is drafting material, not a contract. The controller should adapt it to its own procurement framework, its own contractual structure, and the advice of its own legal function before use.

The language is organised so that the controller selects Pathway 1 or Pathway 2 under framework Section 4.7, applies the corresponding specification at A4.2 or A4.3, and applies the cross-cutting specification at A4.4 to either pathway. The evaluation criteria at A4.5 support assessment of supplier responses against the selected specification.

Bracketed text indicates a value or term the controller must complete. Clause references are local to this annex and should be renumbered to fit the controller's own procurement document. "The Authority" should be replaced with the controller's own designation.

A4.2 Pathway 1 specification: evidence-based outcome assurance

The following clauses specify destruction services that produce, for each storage medium, evidence meeting the eight elements at framework Section 3.2, including a warrant of irretrievability from the party with control of the destruction process that survives reconciliation against the governing terms.

P1.1 Medium-level identification

The Supplier shall record, for each storage medium processed, the manufacturer, model, serial number, capacity, interface and media type, sufficient to distinguish that medium from every other medium processed under this contract, and shall report this identification on the certificate issued for that medium.

P1.2 Method applied and parameters

The Supplier shall record, for each storage medium, the destruction method actually applied to that medium and the parameters of that method, including where applicable the firmware command issued, the verification performed, or the cryptographic erasure sequence executed. Where a method is attempted and falls back to an alternative method, the Supplier shall record both the attempted method and the method actually applied, and shall treat the method actually applied as the method for the purposes of P1.3 and P1.4.

P1.3 Media-appropriate method

The Supplier shall apply, to each storage medium, a method that is capable on the technical evidence of rendering data irretrievable on that medium's media type, and shall be able to evidence the basis on which the method is appropriate to that media type by reference to recognised technical standards applicable to that media type. The Supplier shall not apply a host-issued overwrite method as the sole method on flash-based media, including solid state drives, NVMe devices, embedded multimedia cards and Universal Flash Storage devices.

P1.4 Outcome verification

The Supplier shall verify, for each storage medium, that the method applied achieved the intended outcome on that medium, and shall record the verification result on the certificate. Process completion shall not be recorded or relied upon as outcome verification.

P1.5 Explicit warrant of irretrievability

The Supplier shall provide, on the certificate issued for each storage medium, an explicit warrant that the data on that medium has been rendered irretrievable, with responsibility for that outcome accepted by the Supplier or by the party with control of the destruction process where that party is not the Supplier.

P1.6 Contractual reconciliation

The warrant at P1.5 shall not be disclaimed, contradicted or negated by any licence terms, end user licence agreement, terms of service or other contractual document governing the destruction services or any software used to perform them. Where the Supplier relies on third-party software whose standard terms disclaim outcome responsibility, the Supplier shall procure that the warrant at P1.5 is nonetheless supplied, by the party with control of the destruction process.

A limitation on the amount of the Supplier's financial liability does not of itself breach this clause. The Authority shall specify separately, at [insert], the minimum level of liability it requires in respect of the warranted outcome, and shall evaluate the Supplier's proposed limit against that requirement as a commercial matter rather than as a question of whether a warrant exists.

P1.7 Control and responsibility alignment

The party providing the warrant at P1.5 shall be the party that controls the factors determining the destruction outcome, namely device identification, method selection, enforcement of correct execution, prevention of unsafe alternative methods, and validation of completion. The Authority shall not accept a downstream warranty from an intermediary that does not control those factors as satisfying P1.5.

P1.8 Chain of custody

The Supplier shall document the chain of custody for each storage medium from collection at the Authority's premises to the destruction event, and the disposition of the medium after destruction, including any remarketing, recycling or secure storage.

A4.3 Pathway 2 specification: physical destruction with chain of custody

The following clauses specify destruction services that physically destroy the storage medium to a state appropriate to the media type, with documented evidence of the destruction event, the state achieved, and the chain of custody. Note that P2.6 and P2.7 are not optional extras: without them the arrangement does not meet elements 4 and 8 and does not discharge the obligation, however thorough the rest of the documentation.

P2.1 Media-appropriate physical method

The Supplier shall physically destroy each storage medium by a method that produces a destruction state rendering data on that medium's media type irretrievable, including a particle size or field strength appropriate to that media type. The Supplier shall be able to evidence the basis on which the method is appropriate to the media type by reference to recognised physical destruction specifications applicable to that media type. The Supplier shall not apply a physical destruction standard developed for one media type to a different media type without evidence that it achieves irretrievability on the actual media type.

P2.2 Medium-level documentation

The Supplier shall document each storage medium subjected to physical destruction, identified by serial number or other unique identifier. A record of weight, volume, quantity of equipment or number of collections shall not be accepted as identification of a medium.

P2.3 Destruction event documentation

The Supplier shall document, for each storage medium, the date, time, location and operator of the destruction event. The Authority may require photographic or video evidence of the destruction for media carrying higher-sensitivity data.

P2.4 Chain of custody to destruction

The Supplier shall document the chain of custody for each storage medium from collection at the Authority's premises to the destruction event, including transport, storage and any intermediate handling.

P2.5 Disposition of destroyed material

The Supplier shall document the disposition of the destroyed material, including the recycling or waste disposal route and any further processing of the material that affects the assurance position.

P2.6 Record of the destruction state achieved

The Supplier shall record, for each storage medium or for each destruction run traceable to that medium, the particle size or destruction state actually achieved, and the basis on which that state is appropriate to the media type destroyed. A statement that a medium or a quantity of equipment was destroyed, without the state achieved, shall not be accepted as evidence of the destruction outcome.

P2.7 Explicit warrant and contractual reconciliation

The operator of the destruction process shall state, for each storage medium, that the medium was reduced to the destruction state recorded under P2.6, and shall accept responsibility for that statement. That statement shall not be disclaimed, contradicted or negated by the service contract, terms of business, or any exclusion of responsibility for the destruction outcome. Where the Supplier's standard terms disclaim responsibility for the destruction outcome, the Supplier shall procure that the statement under this clause is supplied.

As at P1.6, a limitation on the amount of the Supplier's financial liability does not of itself breach this clause, and is evaluated against the Authority's separately specified liability requirement.

A4.4 Cross-cutting specification applicable to both pathways

C.1 Definitions

For the purposes of this specification, "storage medium" means the data-bearing component, and not the host device in which it is contained; "irretrievable" means not recoverable using state-of-the-art laboratory techniques; and "warrant" means a statement of outcome with responsibility for that outcome accepted by the party making it.

C.2 Certificate as a deliverable

The certificate or destruction record specified under the selected pathway is a contractual deliverable. The Authority is not obliged to accept, and shall not be deemed to have accepted, a certificate that does not record the elements required under the selected pathway.

C.3 Reporting and audit rights

The Supplier shall report to the Authority on the destruction services at intervals specified by the Authority, and shall permit the Authority, on reasonable notice, to audit the Supplier's destruction process and to require independent verification of the destruction outcome on a sample basis.

C.4 Subcontracting

Where the Supplier subcontracts any element of the destruction chain, including collection, transport, processing, final destruction or downstream remarketing, the Supplier shall remain responsible for the deliverables under this specification and shall procure that the chain of custody and the warrant requirements extend through any subcontracted party.

C.5 No remarketing of unverified media

The Supplier shall not remarket, resell or release into any secondary market any storage medium, or any host device containing a storage medium, until the destruction outcome on that medium has been achieved and evidenced under the selected pathway.

A4.5 Evaluation criteria language

The following criteria support assessment of supplier responses against the selected specification. They are framed so that a response is assessed on whether it produces the evidence the standard requires, rather than on whether the supplier holds accreditations, which validate capability but do not, of themselves, supply the warrant.

CRITERION	WHAT A SATISFACTORY RESPONSE DEMONSTRATES
Medium-level evidence	The supplier's certificate or record identifies the storage medium itself, not only the host device, and records the method applied to that specific medium.
Method appropriateness	The supplier applies methods appropriate to each media type in the Authority's estate, and can evidence the basis on the technical evidence, including for flash-based media.
Outcome evidence	The supplier evidences the outcome on each medium by verification under Pathway 1, or by recording the destruction state achieved under Pathway 2, and does not rely on process completion, or on the fact of physical destruction, as outcome evidence.
Warrant and reconciliation	The supplier provides a warrant from the party with control, and the supplier's governing terms do not disclaim or negate responsibility for the outcome. The Authority reconciles the proposed certificate against the proposed contractual terms before award. This criterion applies to both pathways.
Level of liability	Assessed separately from the warrant. The supplier's proposed limit of liability in respect of the warranted outcome is evaluated against the Authority's stated requirement as a commercial matter. A limit does not determine whether a warrant exists.
Chain of custody	The supplier documents the chain of custody from collection to destruction and the disposition of the medium thereafter.

CRITERION	WHAT A SATISFACTORY RESPONSE DEMONSTRATES
Accreditation in context	Any accreditation the supplier holds is treated as evidence of capability and as an input to supplier management, and is not treated as a substitute for the warrant and outcome evidence required under the selected pathway.

Together with the framework, this reference material supports a DPO in conducting a properly scoped DPIA on end-of-life data destruction, in mapping the controller's current practice against the evidential standard, and in specifying the procurement changes required to discharge the accountability obligation under the selected pathway.

REFERENCES

Sources and primary references

Every proposition in this annex that rests on an external source is drawn from one of the following. Each can be retrieved independently of Data Safe Solutions Ltd.

Legislation

- UK General Data Protection Regulation, in particular Articles 5, 24, 28, 32, 35 and 36.
- Freedom of Information Act 2000, and Freedom of Information (Scotland) Act 2002. The instruments under which the responses analysed at A2 were obtained.
- Cyber Security and Resilience (Network and Information Systems) Bill. Introduced in the House of Commons 12 November 2025; carried over into the 2026-27 session and reintroduced 14 May 2026; Commons report stage and third reading 16 June 2026; Lords first reading 17 June 2026; Lords second reading 14 July 2026; Lords committee stage from 1 September 2026. Not statute at the date of this annex. Bill 4035, bills.parliament.uk. Cited at A1.8.

Technical standards and guidance

- NIST Special Publication 800-88 Revision 2, *Guidelines for Media Sanitization*, September 2025. Supersedes Revision 1 of December 2014. Retains the sanitization programme and the Clear, Purge and Destroy categories, strengthens the treatment of validation, and replaces the technique and tool tables of Revision 1 with a direction to comply with IEEE 2883, NSA specifications, or an organizationally approved standard. Cited at A1.5.
- IEEE 2883-2022, *IEEE Standard for Sanitizing Storage*. Specifies methods for sanitizing logical and physical storage and provides technology-specific requirements and guidance for the elimination of recorded data. Cited at A1.5 and A1.7.
- IEEE 2883.1-2025, *IEEE Recommended Practice for Use of Storage Sanitization Methods*. Provides recommendations for applying the sanitization methods of IEEE 2883 before reuse, resale or disposal.
- NSA/CSS Policy Manual 9-12, *Storage Device Sanitization and Destruction Manual*, and the associated evaluated product specifications, which publish separate requirements for hard disk destruction and for solid state disintegration. Cited at A1.5 and A4.3.
- National Cyber Security Centre guidance on the secure sanitisation and disposal of storage media, which superseded HMG Information Assurance Standard No. 5, *Secure Sanitisation*. Cited at A1.5 and A2.4.

Technical literature

- Michael Wei, Laura M. Grupp, Frederick E. Spada and Steven Swanson, *Reliably Erasing Data from Flash-Based Solid State Drives*, Proceedings of the 9th USENIX Conference on File and Storage Technologies (FAST'11), 2011. The experimental basis for the statement at A1.5 that software overwrite procedures on flash media can report success while leaving data recoverable.

Regulatory correspondence and public authority responses

- Scottish Environment Protection Agency, Freedom of Information response dated 31 March 2026. Cited at A2.5.

- Environment Agency, sequence of Freedom of Information responses between February and May 2026. Cited at A2.5.
- Anonymised Scottish Government body, Freedom of Information (Scotland) Act 2002 response. Cited at A2.4 as illustrating the cryptographic pattern within the Model 3 cohort.

Evidence base

- Freedom of Information programme conducted from January 2026 and live at the date of this annex, asking UK public bodies whether an explicit outcome-based warranty is required following **software-based erasure**, and what recorded evidential assurance is relied upon. Physical destruction was expressly excluded from the scope of the assurance question. 1,036 requests issued; 684 classified responses forming the analysed set; of those, 6 recorded software-based erasure with an explicit outcome warranty, 241 recorded physical destruction and so fell outside the scope of the question, and 437 recorded software-based erasure without an outcome warranty. Each response is a public document held by the authority that issued it, and is individually retrievable through the WhatDoTheyKnow platform. Cited throughout A2.

Note on accreditation schemes

Where this annex refers to industry accreditation and certification schemes, the references are to those schemes in general terms as examples of supplier or product certification. No scheme document is relied upon for any proposition in this annex, and no scheme operator has been consulted on or has endorsed its contents.