DATA SAFE
SOLUTIONS

FRAMEWORK · FOR DATA PROTECTION OFFICERS

A Framework for Conducting a Data Protection Impact Assessment

On end-of-life data destruction, and the evidence required to discharge accountability under Article 5(2) UK GDPR.

> **Advisory, non-commercial, technology neutral and supplier agnostic.**
>
> This framework names no product and no supplier. It is not itself a DPIA and 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 1.4
DOCUMENT VERSION

September 2026
ISSUED

Free to share
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

A Framework for Conducting a Data Protection Impact Assessment on End-of-Life Data Destruction

INTRODUCTION

Purpose, use and status

Purpose of this framework

This framework supports controllers in conducting a Data Protection Impact Assessment specifically scoped to end-of-life data destruction accountability under UK GDPR. It is intended for use by a controller's own Data Protection Officer or equivalent function.

The framework is not itself a DPIA. The DPIA remains the controller's document, conducted by the controller's DPO, recording the controller's specific assessment in respect of the controller's specific processing.

The framework also supports controllers in preparing for the regulatory direction indicated by the Cyber Security and Resilience (Network and Information Systems) Bill. The Bill was introduced in the House of Commons on 12 November 2025, carried over into the 2026-27 session and reintroduced on 14 May 2026 following the King's Speech of 13 May. It completed its Commons stages on 16 June 2026, had its second reading in the House of Lords on 14 July 2026, and entered Lords committee stage on 1 September 2026. It is not statute at the time of writing.

The Bill extends the cyber security regulatory perimeter to relevant managed service providers, brings further categories including data centres within scope, and provides for the designation of critical suppliers to regulated organisations. It does not name the end-of-life IT disposal chain as a regulated category. The direction of travel is nonetheless towards closer regulatory scrutiny of the technology supply chains on which regulated organisations depend. This framework is constructed against the requirements of current UK GDPR rather than against the Bill, and controllers conducting a DPIA using it will be better placed to answer the supply chain assurance questions that regime is likely to generate.

How to use this framework

The framework sets out the methodology a properly scoped DPIA on this processing activity should follow. Section 1 establishes the scope of the assessment and the legal basis on which the DPIA is required. Section 2 identifies the risks the DPIA should assess. Section 3 sets out the assessment criteria. Section 4 addresses the evidential pathways available to discharge the controller's accountability obligation. Section 5 covers consultation requirements. Section 6 addresses documentation and review. Sources and primary references are listed at the end, followed by Annex A.

Each section provides methodological guidance and the substantive considerations a competent DPO should apply when conducting the DPIA in their own organisation. The controller's specific data flows, supplier relationships, and operational circumstances will determine how the framework is applied in any particular case.

> **TWO TESTS, AND THE DIFFERENCE BETWEEN THEM**
>
> A DPIA assesses risk in the ordinary way. It considers likelihood and severity, records the mitigation applied, and states the residual risk that remains after mitigation. Where a high residual risk would remain, Article 36 UK GDPR requires the controller to consult the Information Commissioner before proceeding. This framework does not displace that methodology and nothing in it should be read as doing so.
>
> Separately, and within that assessment, the framework applies a binary test to one question only: destruction assurance. In respect of a specific storage medium, the controller either holds the evidence and the warrant required to demonstrate the destruction outcome, or it does not.
>
> **Risk can be graded. Evidence cannot.**

Status

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

Every proposition in this framework that rests on an external source is referenced, and every source named can be retrieved independently of Data Safe Solutions Ltd.

SECTION 1

Scope of the assessment

1.1 Purpose of the DPIA

A DPIA conducted using this framework assesses the processing activity by which a controller's personal data is destroyed at the end of life of the storage media on which it has been held. The purpose of the assessment is to identify and document the risks to data subjects arising from this processing, to evaluate whether the controller's current arrangements provide sufficient evidence to demonstrate compliance with the controller's accountability obligations under UK GDPR, and to identify the evidential requirements that must be met for the controller to discharge those obligations.

1.2 The fundamental principle

The framework rests on a single definitional premise.

> THE PRINCIPLE
>
> Irrespective of the assurance model in place, irrespective of the service provider engaged, irrespective of the standards referenced or the certifications held, without a warrant of permanent destruction the whole accountability structure falls over.

This is not an analytical position. It is the consequence of the binary nature of the operational reality.

On any storage device, personal data is either permanently irretrievable or it is not. There is no partial destruction, no graded outcome, no acceptable margin of uncertainty. If data can be recovered using state-of-the-art laboratory techniques, destruction has failed.

The controller's accountability obligation under Article 5(2) UK GDPR is to be responsible for, and able to demonstrate, compliance with the principle of integrity and confidentiality at Article 5(1)(f). In the destruction context, that obligation cannot be discharged through process documentation alone. The obligation can only be discharged where the controller holds a warrant that the data on the specific storage medium has been rendered irretrievable.

End-of-life destruction is structurally different from other processing activities in this respect. Once destruction is asserted and the storage medium leaves the controller's possession, the controller has no further operational ability to recover the medium, verify its state, or remediate any failure of destruction that may have occurred. The medium enters the secondary market, the recycling chain, or the disposal chain, and any personal data still present on it is beyond the controller's reach. There is no discrete incident to detect, no breach event to notify, no remediation pathway to invoke. There is only the continuing condition of unknown exposure for the data subjects whose personal data was on the medium.

An "acceptable residual risk" framing is therefore not available to the controller. The accountability question admits of no middle position because the operational reality admits of no middle position. Either the controller holds a warrant of irretrievability for the specific storage medium concerned, or the accountability obligation under Article 5(2) is not discharged.

Responsibility must exist where control exists

The principle has a corollary that runs through every subsequent section of this framework. A warrant of permanent destruction can only be issued by the party that controls the factors determining whether destruction has been achieved: device identification, method selection, enforcement of correct execution, prevention of unsafe alternatives, and validation of completion. Where these factors are controlled by one party and warranted by another, the warrant is structurally conditional even where the conditionality is not stated.

This is corroborated by the account one UK public body has given of its own arrangements. The Scottish Environment Protection Agency, in its formal Freedom of Information response of 31 March 2026, characterised its absence of outcome evidence in respect of personal data destruction as "a gap in our Data Protection Accountability obligations for this processing." SEPA further identified the response it intended to make: "This will be addressed by the drafting of a Data Protection Impact Assessment (DPIA) for the specific processing."

SEPA therefore independently identified both the gap in its own arrangements and the remediation it intended to apply, and that remediation is the one this framework sets out. SEPA is an environmental regulator, not the data protection regulator, and its response is relied on here as a formal account of its own position rather than as an interpretation of UK GDPR.

1.3 The statutory anchor

A DPIA conducted using this framework engages the controller's obligations under a connected set of UK GDPR provisions.

Article 5(1)(f) requires personal data to be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. End-of-life destruction is the moment at which the confidentiality obligation under this principle must be discharged finally, because beyond that point the controller has no further operational ability to protect the data.

Article 5(2) requires the controller to be responsible for, and able to demonstrate, compliance with Article 5(1). This is the accountability obligation. The framework's binary reading sits here.

Article 24 requires the controller to implement appropriate technical and organisational measures and to be able to demonstrate that those measures ensure compliance. This is the positive obligation to put measures in place that actually work, not measures that merely exist.

Article 28 requires the controller to use only processors that provide sufficient guarantees of appropriate technical and organisational measures. Where the controller relies on a destruction supplier acting as a processor, this is the obligation that governs the supplier-side guarantees the controller is entitled to require.

Article 32(1)(d) requires a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing. This is the effectiveness-testing obligation specifically. The framework engages it because the question whether a destruction process has been effective cannot be answered by reference to the existence of the process alone.

Article 36 requires the controller to consult the Information Commissioner prior to processing where a DPIA indicates that the processing would result in a high risk in the absence of measures taken to mitigate that

risk. Where the controller's assessment concludes that a high residual risk remains after the measures identified to mitigate that risk have been applied, Article 36 requires consultation with the Information Commissioner before the relevant processing proceeds.

The Information Commissioner has addressed the relationship between these obligations and destruction certificates directly. In correspondence dated 21 January 2026 (ICO case reference IC-471076-R5B2), the Commissioner stated that a destruction certificate on its own may be a sufficient way to demonstrate compliance only where the controller has ensured that the data has been destroyed effectively. The Commissioner further stated that where disclaimers do not provide the reassurances and confirmations the controller needs to confidently say that data will be destroyed in a way that complies with UK GDPR, the controller should consider using an organisation that does.

The DPIA conducted under this framework therefore proceeds on the basis that the controller must be able to demonstrate, with evidence specific to each storage medium, that the data on that medium has been rendered irretrievable. Where the controller cannot demonstrate this, the obligations at Articles 5(2), 24, 28 and 32(1)(d) are not discharged regardless of the form of the supplier's documentation or the accreditations the supplier holds.

1.4 When a DPIA is required

Article 35 UK GDPR requires a DPIA where processing is likely to result in a high risk to the rights and freedoms of natural persons, having regard to the nature, scope, context and purposes of the processing. Whether the destruction of personal data on end-of-life storage media crosses that threshold is a question the controller must answer on its own circumstances. It is not one this framework can answer universally, and the framework does not assert that every end-of-life destruction activity requires a DPIA as a matter of course.

The processing involves the personal data of all data subjects whose data was held on the storage media. For a typical public sector controller, this includes employees, service users, citizens, patients, customers, suppliers, and other third parties depending on the controller's role and function. The volume and breadth of personal data potentially affected is substantial.

Two features of this processing bear on the screening decision. The first is conventional: the volume, sensitivity and categories of personal data involved. The second is specific to destruction and is set out at 1.2 above: the processing is irreversible if it fails, and the controller has no operational pathway to detect or remediate the failure once the medium has left its possession.

For controllers whose end-of-life media routinely contains large-scale special category data, criminal offence data, data relating to vulnerable individuals, or comparable high-risk information, Article 35 screening is likely to identify a requirement for a DPIA. Other controllers should apply the Article 35 screening test to their own circumstances. Where doubt remains, the Information Commissioner's guidance is that a DPIA should be conducted.

The empirical position across the UK public sector supports this characterisation. Between January and May 2026, 1,036 Freedom of Information requests were issued to UK public bodies asking what recorded evidence is held that personal data on disposed storage media was actually rendered irretrievable.

1,036	684	437
requests issued to UK public bodies	substantive responses received	held no outcome warranty and no device-level evidence

The responses, now on the public record, show that the substantial majority hold only supplier process certificates and do not hold device-level outcome evidence. The architectural gap is present across central government, the NHS, devolved administrations, regulators, and local authorities.

Findings as at 22 May 2026. Each response is a public document held by the authority that issued it and can be retrieved independently.

1.5 Processing activity to be assessed

The DPIA should assess the destruction of personal data on storage media at the end of life of the host device or of the storage media itself. This includes:

1. Personal data held on storage media within end-of-life IT equipment (desktops, laptops, servers, tablets, mobile devices, networked storage devices, multifunctional devices and any other equipment containing data-bearing components).
2. Personal data held on standalone storage media at end of life (external drives, USB devices, removable media, backup media).
3. Personal data held on storage media being repurposed, reassigned or returned, including media transferred between data controllers within a group structure or to a different operational context.

The DPIA should cover all steps from the point at which the storage medium is identified as having reached end of life to the point at which the controller's accountability obligation in respect of the data on that medium is discharged.

1.6 Data categories to be considered

In conducting the DPIA, the controller's DPO should identify the categories of personal data potentially present on end-of-life storage media in their organisation. Depending on the controller's function and the role of the specific equipment, these are likely to include:

1. Employee personal data including HR records, payroll information, contact details, performance records, disciplinary records, and occupational health information.
2. Service user, citizen, patient, customer or claimant personal data, including identification details, contact information, service records, financial information, and correspondence.
3. Special category personal data under Article 9 UK GDPR, including health data, data concerning racial or ethnic origin, religious or philosophical beliefs, trade union membership, biometric data, and data concerning sexual orientation, where the controller's function involves the processing of such data.
4. Personal data relating to criminal convictions and offences under Article 10 UK GDPR, where the controller's function involves the processing of such data.

5. Personal data of third parties incidentally captured (witnesses, contacts, professional advisors, family members) where present in the records held by the controller.

6. Personal data held in unstructured form (email archives, document drafts, cached content, browser history, application data) which may be present on storage media even where the device's primary function does not involve formal record-keeping.

The DPIA should proceed on the basis that personal data of multiple categories is likely to be present on any item of end-of-life storage media unless the controller can specifically demonstrate otherwise.

1.7 Data subjects to be considered

The data subjects to be considered in the DPIA are all individuals whose personal data is or may be present on the storage media being processed. The number of data subjects affected by any given item of storage media is not knowable in advance and may be substantial. The DPIA should proceed on the basis that a typical end-of-life storage medium in a public sector controller may contain the personal data of hundreds or thousands of individual data subjects.

1.8 Operational and temporal scope

The temporal scope of the DPIA is the operational life cycle of end-of-life storage media from identification through to discharge of the controller's accountability obligation. The DPIA is intended to be evergreen rather than tied to a specific equipment refresh cycle, on the basis that end-of-life processing is continuous in any controller with an ongoing operational IT estate.

The operational scope should include all storage media types in current use by the controller, including but not limited to: hard disk drives (HDDs), solid state drives (SSDs), non-volatile memory (NVMe) devices, embedded multimedia cards (eMMC), Universal Flash Storage (UFS), removable media, and any future storage media types that may enter the controller's estate. The DPIA should be media-type-neutral on the basis that the accountability obligation under Article 5(2) is media-type-neutral. The framework does not, however, treat all methods of destruction as equivalent across media types; the assessment criteria in Section 3 address the question of whether the method applied is appropriate to the specific media type.

The geographical scope of the DPIA is the United Kingdom. Where the controller's operations or supply chain extends outside the United Kingdom, additional considerations under Articles 44 to 50 UK GDPR may apply but are outside the scope of this framework.

1.9 Out of scope

The following are out of scope for a DPIA conducted using this framework:

1. Live data backup and archive operations during the operational life of the device. These are covered by separate processing activities and separate assessments.

2. Decommissioning of services, applications or systems, where the underlying storage media remains in operational use. These are covered by separate change management processes.

3. Personal data destruction in paper or other non-digital form. These are subject to separate destruction methodologies and are not addressed by this framework.

4. Destruction of non-personal data on end-of-life storage media. The framework focuses on personal data because that is where the Article 5(2) accountability obligation applies. Controllers may have separate destruction obligations in respect of other categories of data, including commercially sensitive information, classified information and intellectual property, which are not addressed here.

SECTION 2

Risks to be assessed

2.1 The function of risk identification under the fundamental principle

The DPIA identifies and assesses risk in the ordinary way, applying the controller's own methodology. Section 2.7 addresses how the register is scored and how residual risk is recorded. This section addresses what belongs in the register.

The fundamental principle established at Section 1.2 governs one part of that exercise. Where the question is whether the controller can demonstrate a warrant of irretrievability for a specific storage medium, the answer does not admit of a grade. Either the evidence is held or it is not.

The risks set out in this section are therefore framed as the categories of consequence that follow from the controller being unable to demonstrate that warrant. The DPIA should identify each risk that is relevant to the controller's circumstances and establish, for each, whether the controller holds the evidence required to close it out for the specific storage medium concerned.

2.2 Risks to data subjects

The DPIA should identify the risks to data subjects whose personal data is or may be present on end-of-life storage media. These risks are independent of the controller's intentions, supplier arrangements, or operational practices. They are properties of the data itself once it has left the controller's operational reach. The DPIA should consider:

1. **Risk of recovery of personal data by an unauthorised party.** Storage media that has not been verifiably purged retains data that can be recovered by any party with access to the medium and the technical means to extract it. The data subjects affected have no control over and no awareness of this exposure.

2. **Risk of indefinite duration of exposure.** Unlike a discrete breach event with a defined exposure window, undetected destruction failure creates an exposure that continues for the operational life of the storage medium in third-party possession. The data subjects affected cannot be notified because the exposure cannot be identified, dated, or scoped.

3. **Risk to special category and criminal conviction data.** Where personal data of the categories identified at Article 9 and Article 10 UK GDPR is present on the storage media, the consequences of recovery are correspondingly more serious. Health data, biometric data, criminal records, religious affiliations, and similar categories carry direct safeguarding implications for the data subjects if recovered by an unauthorised party.

4. **Risk to data subjects who are vulnerable, identifiable, or otherwise specifically exposed.** For controllers whose data subjects include children, victims of crime, witnesses, individuals with safeguarding concerns, individuals in fear of identification, or others whose personal circumstances mean that data recovery would cause specific and disproportionate harm, the risk register should record these specifically. The DPIA should identify whether such data subjects are likely to be present in the data held on end-of-life storage media.

5. **Risk of secondary harm from data combination.** Personal data recovered from end-of-life storage media may be combined with personal data from other sources to enable harms, including identity theft, fraud, targeted attack and stalking, that the individual fields of data would not enable in isolation. The DPIA should consider the categories of data likely to be present and the combinatorial harm risk.

2.3 Risks to discharge of the controller's accountability obligation

The DPIA should identify the risks that, regardless of operational practice, the controller will be unable to demonstrate discharge of the accountability obligations under Articles 5(2), 24, 28 and 32(1)(d) UK GDPR in respect of any specific storage medium that has left the controller's possession. The DPIA should consider:

1. **Risk of inability to identify the specific storage medium.** Where the controller's records do not associate destruction events with specific items of storage media, by serial number or other unique identifier, the controller cannot demonstrate that any particular medium has been the subject of any particular destruction event. The accountability question is asked at the level of the specific medium, not at the level of the destruction batch.

2. **Risk of inability to identify the destruction method applied.** Where supplier certification records the methodology of the destruction service in general terms but does not record which method was applied to the specific storage medium, the controller cannot demonstrate that the method applied was appropriate to the media type concerned.

3. **Risk of inability to evidence outcome verification.** Where the certification confirms that a process was followed but does not record that the outcome was verified, the controller has no record that the data was actually rendered irretrievable. Process completion is not equivalent to outcome verification. A process can complete with the data still recoverable.

4. **Risk of inability to evidence the chain from destruction event to certificate issuance.** Where the certificate is issued by the destruction supplier but the controller holds no evidence linking the certificate to a specific destruction event for a specific medium, the certificate's evidential value in respect of the specific medium is limited.

5. **Risk of inability to evidence the chain of custody before destruction.** Where the destruction event is documented but the period between the medium leaving the controller's possession and the destruction event is not evidenced, the controller cannot demonstrate that the data was not exposed during transit, storage at supplier facilities, or other intermediate handling.

6. **Risk of inability to satisfy the Article 32(1)(d) effectiveness-testing obligation.** Where the destruction methodology generates documentation of process but not documentation of outcome, the controller cannot evidence that the technical and organisational measures in place are effective. Article 32(1)(d) requires testing, assessment and evaluation of effectiveness. A certificate that records process completion without outcome verification does not satisfy this obligation.

2.4 Risks specific to methodological adequacy

Even where evidence exists that a particular method was applied to a particular medium, the DPIA should consider whether the method is one that is capable, on the technical evidence, of rendering the data irretrievable on the media type concerned. The DPIA should consider:

1. **Risk of methodological inadequacy on flash storage.** Methodologies developed for magnetic media, meaning overwrite-based approaches, do not, on the technical evidence, reliably destroy data on flash storage media. Wear levelling, over-provisioning, and bad-block remapping mean that an overwrite operation may leave cells containing earlier writes intact and recoverable. NIST SP 800-88 distinguishes between Clear, Purge and Destroy level operations and, at Revision 2, directs organisations to IEEE 2883, NSA specifications or another approved standard for technique-level requirements. IEEE 2883-2022 specifies methods for sanitizing logical and physical storage and provides technology-specific requirements for the elimination of recorded data, including on flash media. Where a controller's destruction supplier applies an overwrite-based methodology to flash storage, the methodology itself may not deliver the outcome the certificate asserts.

2. **Risk of methodology fallback recorded on the certificate.** A destruction process may attempt a higher-assurance method, such as a Purge-level command, and, where the command is unsupported by the device firmware or fails on the device, fall back to a lower-assurance method, such as a Clear-level overwrite. The destruction certificate may record both attempts, with the higher-assurance method shown as failed and the lower-assurance method shown as completed. The DPIA should consider whether the controller is in a position to read such certificates accurately and whether the actual method applied, as distinct from the method attempted, meets the evidential standard at Section 3.

3. **Risk of methodological inadequacy from partition and format operations.** Operations that remove the file system structure of the storage medium, including partition, format and reset operations, without overwriting the underlying data leave the data recoverable using standard forensic recovery tools. Such operations are not destruction methodologies and do not discharge the Article 5(2) obligation in any context.

4. **Risk of remapped sectors not being addressed.** Storage media that has accumulated remapped sectors during operational life may have data resident in those sectors that is not addressed by a host-issued overwrite operation. Where destruction certificates record successful overwrite of host-addressable space but do not address remapped sectors, the residual data risk persists.

5. **Risk of methodological inadequacy from physical destruction without medium-appropriate process.** Physical destruction methodologies are not uniformly effective across all media types. Shred particle sizes developed for hard disk drives do not reliably render data irrecoverable on solid state media, where an intact memory package surviving the shredder is a recoverable medium in a smaller housing. The DPIA should consider whether the physical destruction methodology applied is appropriate to the media types being destroyed, and whether the destruction record states the particle size or destruction state actually achieved.

6. **Risk of reliance on key reference deletion as a destruction method.** Where the controller relies on the deletion of an encryption key as the means of rendering personal data irretrievable, the DPIA should distinguish between destruction of the key material itself and deletion of a stored or escrowed copy of a key. Cryptographic erasure, where personal data has been encrypted throughout its life on the medium and the key material is itself verifiably and completely destroyed, and cryptographic scramble, where the on-device key is rotated and destroyed at the hardware level so that the existing ciphertext is permanently orphaned, are each capable, on the technical evidence, of rendering data irretrievable, because the key material that could return the ciphertext to readable form no longer exists.

   Deletion of a key reference is not equivalent. Where what has been deleted is a stored or escrowed copy of a key protector, for example a recovery key held in a directory service or cloud tenant, and a logged record confirms that the deletion action occurred, the controller holds evidence that an administrative action was performed. It does not hold evidence that the data has been rendered irretrievable. The ciphertext remains intact on the medium, other key protectors may persist, and the deleted copy may itself have been backed up before deletion. Encryption protects data at rest during the operational life of the device. The deletion of a key reference does not discharge the end-of-life obligation to render the data irretrievable.

7. **Risk of process compliance with HMG sanitisation guidance being treated as discharge of the controller's accountability obligation.** UK government sanitisation guidance, including the predecessor HMG IA Standard No. 5, is process-oriented and does not require the controller to hold device-level outcome evidence supported by an explicit warrant of irretrievability. A controller whose internal procedures and supplier specifications are aligned to that guidance is therefore compliant with the guidance without necessarily being compliant with the controller's separate accountability obligation under UK GDPR. The DPIA should consider whether the controller has treated process compliance under that guidance as discharge of the UK GDPR obligation. Where this is the case, the finding is that process compliance does not, of itself, satisfy the evidential standard at Section 3, and the framework's methodology applies regardless of the controller's position under the guidance. The two regimes operate independently and the controller must satisfy each on its own terms.

To rely on a cryptographic method as discharging the obligation, the DPIA should establish that the controller holds evidence of each of the following:

(a) that the key material itself has been destroyed, and that destruction verified, rather than a record that a deletion action was performed;

(b) that no other copy of the key, and no other key protector capable of returning the ciphertext to readable form, survives in any directory service, cloud tenant, key management system, escrow, backup or recovery store; and

(c) that the medium was encrypted in full from first use, such that no personal data was written to the medium in unencrypted form before encryption was enabled and no personal data resides outside the encrypted volume.

Where the controller cannot evidence each of (a), (b) and (c), the cryptographic method relied upon does not meet the evidential standard at Section 3, and the finding is recorded accordingly.

2.5 Supply chain risks

The DPIA should identify the risks introduced by the controller's reliance on third-party suppliers, typically IT Asset Disposition providers, destruction services, or software vendors operating destruction tooling, in the destruction chain. The DPIA should consider:

1. **Risk that the supplier certificate does not constitute evidence of outcome.** A supplier certificate that records the supplier's process having been followed is evidence that the supplier carried out their process. It is not, of itself, evidence of the outcome on the specific storage medium. The DPIA should consider whether the supplier's certificate, as currently formatted, satisfies the controller's evidential requirements.

2. **Risk that the supplier's contractual position disclaims the outcome the certificate appears to assert.** Many destruction software products are supplied under licence terms that explicitly disclaim responsibility for the destruction outcome, exclude liability for data loss, and cap liability to the licence fee paid. Where a certificate issued by such software appears to assert successful destruction while the governing licence terms deny outcome responsibility, the certificate's evidential value collapses on reconciliation. The DPIA should consider whether the supplier's certificates survive reconciliation against the governing licence terms.

3. **Risk that downstream warranties from the controller's immediate supplier do not address upstream disclaimers.** Where a controller's immediate supplier, typically an ITAD, provides a warranty of destruction to the controller, but the underlying destruction software disclaims the outcome, the ITAD's warranty is structurally conditional regardless of how it is presented. The ITAD does not control the software's internal operation and cannot warrant what the software does not warrant. The DPIA should consider whether any warranty provided by the controller's immediate supplier is supported by an equivalent warranty from the supplier of the destruction tooling.

4. **Risk of supplier subcontracting.** Where the supplier subcontracts elements of the destruction chain to third parties, including collection, transport, processing, final destruction and downstream remarketing, the controller's accountability obligation is not subcontracted. The DPIA should consider whether the controller holds evidence of the full chain of custody and processing through any subcontracted parties.

5. **Risk of supplier remarketing of media.** Where the supplier operates a remarketing channel for end-of-life equipment, storage media may enter the secondary market after the destruction process. The DPIA should consider whether the supplier's remarketing process verifies the destruction outcome on each specific medium before remarketing, or whether remarketed media may carry data that has not been verifiably destroyed.

6. **Risk of supplier certificate scope mismatch.** Where the supplier certificate refers to a "unit", typically the host device such as a desktop or laptop, rather than to the data-bearing component, meaning the storage medium within the unit, the certificate's evidential scope may not extend to the storage medium itself. The DPIA should consider whether supplier certificates address the data-bearing component specifically or address only the host device.

7. **Risk that supplier accreditation is treated as outcome responsibility.** Industry accreditations and certifications validate that the supplier or product meets defined criteria under defined conditions. They do not, of themselves, demonstrate that the outcome on any specific storage medium has been verified, and the certifying bodies do not accept outcome responsibility. The DPIA should consider whether the controller's reliance on supplier accreditation has been confused with reliance on outcome warranty.

2.6 Risks to forward compliance

The DPIA should identify the risks the controller faces from emerging regulatory direction beyond current UK GDPR. The DPIA should consider:

1. **Risk of non-alignment with the direction of the Cyber Security and Resilience Bill.** The Bill extends the cyber security regulatory perimeter to relevant managed service providers, brings further categories including data centres within scope, and provides for the designation of critical suppliers to regulated organisations. It does not name the end-of-life IT disposal chain as a regulated category, and a disposal service does not automatically satisfy the definition of a managed service. The direction of travel is nonetheless towards closer regulatory scrutiny of the technology supply chains on which regulated organisations depend. Controllers whose current arrangements rely on process-based supplier certification without device-level outcome evidence should consider how those arrangements would answer supply chain assurance questions asked under such a regime.
2. **Risk of evolving ICO enforcement focus.** The accountability principle under Article 5(2) is the subject of continuing regulatory development. Controllers whose current arrangements predate the focus on outcome-evidence-based accountability may face questions in any future enforcement engagement that current arrangements were not designed to answer.
3. **Risk of misalignment with EU GDPR for cross-border operations.** Where the controller's data flows or operations involve EU jurisdictions, the EU GDPR accountability obligation under Article 5(2) creates equivalent or stronger requirements. Controllers with EU exposure should consider whether their destruction arrangements satisfy both regimes.

2.7 Risk register output

The output of the risk identification stage of the DPIA is a register of the risks identified at 2.2 through 2.6 above that are applicable to the controller's circumstances.

The register should be scored in accordance with the controller's own DPIA methodology, recording likelihood and severity for each risk and, following the mitigation identified in Section 4, the residual risk that remains. Where the controller's assessment is that a high residual risk would remain, Article 36 UK GDPR requires consultation with the Information Commissioner before the processing proceeds.

The scoring does not extend to the evidential question. Whether the controller holds, for a specific storage medium, the evidence and the warrant set out at Section 3.2 is a matter of fact and is recorded as met or not met. The function of the subsequent sections of the DPIA is to establish which is the case for each combination of supplier and media category, and to identify the mitigation that closes any gap.

SECTION 3

Assessment criteria

3.1 The function of assessment under the fundamental principle

The assessment stage of the DPIA evaluates the controller's current evidential position against the requirements established in Section 1 and the risks identified in Section 2. The assessment is an evidence audit, not a risk score. For each combination of supplier, storage media category, and destruction method in the controller's process, the assessment establishes whether the evidence the controller holds amounts to a warrant of permanent destruction for the specific storage media concerned.

Where the warrant exists in evidence terms, the assessment records this and the basis. Where the warrant is absent, the assessment records the specific gap and identifies it as a finding the DPIA must address through mitigation under Section 4. The assessment does not record partial discharge of the obligation because the operational reality does not admit of partial discharge.

3.2 The evidential standard

The evidential standard for discharge of the obligation in respect of any specific storage medium is the controller's ability to demonstrate, with reference to specific recorded evidence and a warrant of irretrievability supplied by the party with control of the destruction process, that the personal data on that specific medium has been rendered irretrievable.

The evidence required to meet this standard comprises the following eight elements.

1. **Identification of the specific medium.** Evidence that uniquely identifies the storage medium concerned, by manufacturer, model, serial number, capacity, or other unique identifier, and distinguishes it from all other media subject to the same destruction process.

2. **Identification of the destruction method applied.** Evidence that records the specific destruction method applied to the specific medium, including the parameters of the method (overwrite passes, purge commands issued, physical destruction process and state achieved, cryptographic erasure sequence) sufficient to enable independent verification that the method was capable of achieving the asserted outcome.

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 the media type concerned. This may be established by reference to recognised technical standards, such as the Purge level defined in NIST SP 800-88 and the technology-specific sanitization methods specified in IEEE 2883-2022, but the evidence must address the specific media type.

4. **Verification of the destruction outcome.** Evidence that the method, having been applied, achieved the intended outcome on the specific medium. This may be by means of read-back verification, cryptographic verification of key-material destruction, a recorded destruction state for physically destroyed media, a certificate from an independent verification process, or other recorded evidence specific to the medium concerned.

5. **Chain of custody before and after destruction.** Evidence that the medium remained in controlled custody between leaving the controller's operational use and the destruction event, and that the medium did not leave controlled custody between the destruction event and final disposal or remarketing without the destruction outcome being verified.

6. **Date and time of destruction.** Evidence that records when the destruction event occurred, sufficient to enable correlation with the controller's asset records and the supplier's process records.

7. **Identification of the party effecting destruction.** Evidence that records the identity of the party that carried out the destruction, sufficient to enable accountability tracing if questions subsequently arise.

8. **An explicit warrant of irretrievability supplied by the party with control of the destruction process.** A statement, on the certificate or in an accompanying contractual document that survives reconciliation against any governing licence terms or service contract, that the data on the specific medium has been rendered irretrievable, with responsibility for that outcome accepted by the party making the statement. This is the warrant that the fundamental principle at Section 1.2 requires.

The evidential standard is met when the controller holds, in respect of any specific storage medium, evidence on each of elements 1 to 8. Where any element is missing, the standard is not met.

> THE RECONCILIATION TEST
>
> Element 8 is structural. A certificate that asserts a successful outcome while the governing licence terms or service contract disclaim responsibility for that outcome is not a warrant. The disclaimer prevails on reconciliation. This test applies to every assurance model in this framework without exception, and it applies to physical destruction contracts on the same terms as to software licences.
>
> The test looks for accepted responsibility, not for the size of the remedy attached to it. A term that removes responsibility for the destruction outcome defeats element 8. A financial limit on the liability flowing from that responsibility does not, by itself, negate the warrant: a supplier that states the data has been rendered irretrievable, accepts responsibility if it has not, and caps the resulting remedy at a stated sum has still given a warrant. Whether that limit is adequate is a commercial and risk question for the controller, recorded separately in the DPIA, and is not part of the evidential standard.

3.3 The three assurance models

End-of-life destruction practice in the UK can be characterised at three assurance models, each with distinct evidential properties relative to the standard at 3.2. The models are descriptive of current sector practice and are derived from the substantive evidence base across the 684 substantive FOI responses received from UK public sector controllers.

> **Model 1: Evidence-based outcome assurance**
>
> Destruction practice in which the certificate produced records each of the elements at 3.2 and includes an explicit warrant of irretrievability supplied by the party with control of the destruction process, surviving reconciliation against any governing licence terms. The medium is identified specifically. The method is recorded with parameters. The method is demonstrably appropriate to the media type. The

outcome is verified. The chain of custody is recorded. The date and identity of the destruction event are recorded. A warrant is supplied.

The certificate constitutes evidence sufficient to discharge the obligations at Articles 5(2), 24, 28 and 32(1)(d) in respect of the specific medium.

Model 2: Physical destruction with chain of custody

Destruction practice in which the medium is physically destroyed, by shredding, crushing, disintegration, degaussing where the media type permits, or otherwise rendered physically inoperable, to a particle size or destruction state appropriate to the media type, with documented evidence of the destruction event and the chain of custody from the controller to the destruction point.

Physical destruction is frequently treated as self-evidently sufficient. Under this framework it is not. Elements 1, 2, 3, 5, 6 and 7 are met by direct documentation where the destruction record identifies the specific medium. Element 4, outcome verification, is met where the record states the particle size or destruction state actually achieved and that state is appropriate to the media type. Element 8, the warrant, is met where the operator of the destruction process states, in terms that survive reconciliation against the governing service contract, that the specific medium was reduced to that state, and accepts responsibility for that statement.

Model 2 is therefore subject to the same two tests as Model 1: the outcome must be recorded rather than assumed, and the warrant must survive reconciliation. Two failure modes are common and both should be tested in the DPIA. The first is media-type mismatch, where shred particle sizes developed for hard disk drives are applied to solid state media and leave intact memory packages. The second is contractual, where physical destruction service contracts contain the same outcome disclaimers found in destruction software licences, declining responsibility for whether data has in fact been rendered irretrievable. Where they do, the reconciliation test fails on a Model 2 arrangement exactly as it fails on a Model 3 arrangement. A cap on the financial remedy is a separate matter and does not, by itself, defeat the element.

Model 2 satisfies the obligations at Articles 5(2), 24, 28 and 32(1)(d) in respect of the specific medium where the destruction methodology is appropriate to the media type, the state achieved is recorded, the chain of custody is complete, and the warrant survives reconciliation. Where any of those is absent, Model 2 does not discharge the obligation.

Model 3: Process-based assurance

Destruction practice in which the supplier produces a certificate recording that a process was followed, without recording the elements at 3.2 in respect of the specific storage medium and without a warrant of irretrievability that survives reconciliation against the governing licence terms. The certificate may reference the host device rather than the storage medium. The certificate may reference the destruction methodology in general terms rather than recording which method was applied to which medium. The certificate may include accreditation references that demonstrate the supplier operates a controlled process.

The certificate does not, by its contents, evidence that the data on each specific storage medium has been rendered irretrievable, and does not carry the warrant that the fundamental principle requires.

Model 3 is the dominant practice in the UK public sector. Of the 684 substantive FOI responses received across central government, the NHS, devolved administrations, regulators and local authorities, 437 confirmed arrangements that hold no outcome warranty and no device-level evidence. The Scottish Environment Protection Agency's characterisation of its own arrangements as containing "a gap in our Data Protection Accountability obligations" is one public body's own account of what Model 3 amounts to in evidential terms.

3.4 Mapping current practice to the three models

The DPIA should establish, for each combination of supplier and storage media category in the controller's destruction process, which model currently applies. The mapping should be evidence-based, not aspirational. Where the controller's supplier holds accreditations and follows controlled processes, this does not by itself place the practice at Model 1 or Model 2. The relevant question is what evidence the controller holds in respect of each specific storage medium, examined against the requirements at 3.2.

In conducting the mapping, the DPIA should:

1. **Obtain specimen certificates from each destruction supplier.** The controller's DPO should request specimen destruction certificates from each supplier the controller uses, covering each category of storage media processed. Where the certificates produced in operational practice differ from the supplier's documented specimen, the operational certificates are the relevant evidence.

2. **Obtain the governing licence terms and service contracts.** The controller's DPO should obtain the supplier's standard licence terms, end user licence agreement, terms of service, and any other contractual documents that govern the supplier's responsibility for the destruction outcome. The reconciliation test at 3.2 element 8 requires these documents to be examined alongside the certificate. This applies equally to physical destruction service contracts.

3. **Examine each specimen against the requirements at 3.2.** For each specimen, the DPIA should determine which of the eight evidential elements are present, which are absent, and which are present in general terms but not specific to the storage medium. The reconciliation between the certificate's assertions and the contractual disclaimers should be recorded specifically.

4. **Establish whether the certificates can in principle satisfy the standard.** Some certificates may be capable of meeting the standard at 3.2 with additional supplier documentation or specification changes. Others may be structurally incapable of meeting it, either because the certificate format does not record the necessary elements or because the governing contractual terms disclaim the outcome responsibility the warrant would require.

5. **Record the result for each supplier and media category.** The output of the mapping is a record, for each combination of supplier and media category, of the model currently in operation.

3.5 The assessment finding

Following the mapping at 3.4, the DPIA should record an assessment finding for each combination of supplier and media category in the controller's destruction process. The finding takes one of three forms.

Finding A: Evidential standard met (Model 1 or Model 2). The controller holds, in respect of each specific storage medium passing through the destruction process with this supplier and in this media category,

evidence sufficient to demonstrate discharge of the accountability obligations. The DPIA records the evidential basis and notes that no further mitigation is required for this combination.

Finding B: Evidential standard not met but supplier capable. The controller's current arrangements with this supplier do not meet the standard at 3.2, but the supplier is capable of producing certificates that would meet the standard, with a warrant that survives reconciliation against the governing terms, if the controller specified the requirement. The DPIA identifies the specification update required and the contractual changes necessary to put the warrant in place.

Finding C: Evidential standard not met and supplier not capable. The controller's current arrangements with this supplier do not meet the standard at 3.2, and the supplier does not have the capability or the contractual willingness to produce certificates that would meet it with a warrant surviving reconciliation. The DPIA identifies that a supplier change or process change is required to discharge the obligation.

The DPIA should record the finding for each combination clearly. Where the standard is not met, the DPIA should not soften the finding. Under the fundamental principle established at Section 1.2, the obligation is either discharged or it is not. A finding that the standard is partially met, broadly aligned, or substantively compliant is not a finding that the standard is met.

SECTION 4

Evidential pathways and mitigation

4.1 The function of mitigation under the fundamental principle

Where the assessment in Section 3 records a Finding B or Finding C in respect of any combination of supplier and media category, the DPIA must identify the mitigation required to bring the controller's evidential position into compliance with the standard at 3.2. Mitigation of the evidential gap is not a matter of reducing risk to an acceptable level. The gap is closed or it is not. After mitigation the controller either holds a warrant of permanent destruction for each specific storage medium passing through the destruction process, or the mitigation is incomplete. The controller's wider risk treatment, including the recording of residual risk and any consultation required under Article 36 UK GDPR, proceeds in accordance with the controller's own DPIA methodology.

This section sets out the evidential pathways available to the controller and what each requires. The controller's choice of pathway is a matter for the controller's own decision-making, having regard to operational, financial, environmental and reputational considerations. The framework does not prescribe the pathway. The framework prescribes only that the pathway selected, when implemented, must produce the warrant the fundamental principle requires.

4.2 Pathway 1: Evidence-based outcome assurance (Model 1)

This pathway closes the evidential gap by obtaining destruction services that produce certificates meeting the standard at 3.2, including a warrant of irretrievability supplied by the party with control of the destruction process and surviving reconciliation against any governing licence terms. Specification requirements for this pathway include:

1. **Specific medium identification on the certificate.** The supplier must record the manufacturer, model, serial number, capacity, interface and media type of each storage medium destroyed.
2. **Specific method identification on the certificate.** The supplier must record the destruction method applied to each specific medium, including the parameters of the method.
3. **Media-appropriate method.** The supplier must apply a method appropriate to the media type, supported by evidence that the method is capable of rendering data irretrievable on that media type.
4. **Outcome verification.** The supplier must verify the destruction outcome on each specific medium and record the verification result on the certificate.
5. **Explicit warrant of irretrievability.** The certificate must include an explicit warrant that the data on the specific medium has been rendered irretrievable, with responsibility for that outcome accepted by the party issuing the warrant.

6. **Reconciliation of certificate and contractual position.** The warrant on the certificate must not be disclaimed, contradicted or negated by the governing licence terms, end user licence agreement, or service contract. A limit on the amount of the supplier's financial liability does not of itself breach this requirement; the controller should specify the minimum level of liability it requires separately, and evaluate the supplier's proposed limit against it as a commercial matter. Where the supplier's standard contractual documents disclaim outcome responsibility, the controller's procurement specification must require the supplier to issue contractual documents that align with the warrant on the certificate. A warrant on a certificate that is contradicted by the licence terms does not survive reconciliation and does not satisfy the standard.

7. **Control-and-responsibility alignment.** The party warranting the outcome must be the party that controls the factors determining outcome: device identification, method selection, enforcement of correct execution, prevention of unsafe alternatives, and validation of completion. Where these factors are controlled by one party, typically the software vendor, and warranted by another, typically the ITAD, the warrant is structurally conditional. The controller's specification must require the warrant to be supplied by the party with control.

8. **Chain of custody documentation.** The supplier must document the chain of custody from the controller's premises to the destruction event, and the disposition of the medium after destruction, whether remarketing, recycling or secure storage.

Where the controller's existing supplier is not currently producing certificates that meet these requirements but is capable of doing so with a specification update, the DPIA identifies the specification update as the mitigation. Where the existing supplier is not capable, the DPIA identifies that a supplier change is required. The pathway produces a certificate that, examined against the standard at 3.2 and reconciled against the governing contractual documents, demonstrates discharge of the accountability obligations in respect of each specific storage medium.

4.3 Pathway 2: Physical destruction with chain of custody (Model 2)

This pathway closes the evidential gap by physically destroying the storage medium and documenting the destruction event, the destruction state achieved, and the chain of custody to the standard at 3.2. Specification requirements for this pathway include:

1. **Physical destruction methodology appropriate to the media type.** The destruction methodology must produce particle sizes or destruction states that render data on the specific media type irretrievable. Media-type-specific physical destruction requirements are set out in NSA/CSS Policy Manual 9-12 and the associated evaluated product specifications, which publish separate requirements for hard disk destruction and for solid state disintegration. UK organisations should also have regard to NCSC guidance on the secure sanitisation and disposal of storage media, which in heightened circumstances specifies destruction to particles of 6mm or less with the resulting particle size verified. Particle sizes specified for hard disk drives must not be applied to solid state media without separate justification.

2. **Record of the destruction state achieved.** The supplier must record, for each medium or each destruction run traceable to the 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 equipment was destroyed, without the state achieved, does not satisfy element 4 at 3.2.

3. **Documentation of the specific medium destroyed.** The supplier must document each storage medium subjected to physical destruction, identified by serial number or other unique identifier.

4. **Documentation of the destruction event.** The supplier must document the date, time, location and operator of the destruction event for each medium. Photographic or video evidence of the destruction may be appropriate in higher-sensitivity contexts.

5. **Chain of custody from controller to destruction point.** The supplier must document the chain of custody for each medium from the controller's premises to the destruction event, including transport, storage, and any intermediate handling.

6. **Explicit warrant and contractual reconciliation.** The operator of the destruction process must state that the specific medium was reduced to the recorded destruction state, and accept responsibility for that statement. The service contract and terms of business must be examined alongside that statement. Where the contract disclaims responsibility for the destruction outcome, the warrant does not survive reconciliation and the standard is not met. A limit on the amount of the operator's financial liability is assessed separately, as at 4.2.

7. **Disposition of destroyed material.** The supplier must document the disposition of the destroyed material, including the recycling stream or waste disposal route, and any further processing of the destroyed material that affects the assurance position.

> WHERE THE WARRANT COMES FROM UNDER THIS PATHWAY
>
> The warrant is not supplied by the fact of physical destruction. It is supplied by the operator of the destruction process, in a statement that the specific medium was reduced to a recorded destruction state appropriate to its media type, with responsibility for that statement accepted and not disclaimed by the governing service contract. The chain of custody documentation evidences that the medium was within controlled custody from the controller's premises to that point.
>
> Where the state achieved is recorded, the methodology is appropriate to the media type, the chain of custody is complete and the warrant survives reconciliation, the obligation is discharged. Where the controller holds only a certificate of collection, a weight ticket, or a statement that a quantity of equipment was destroyed, none of those is a warrant and the obligation is not discharged.

This pathway destroys asset value. The medium cannot be remarketed because it no longer exists. The pathway is appropriate where the controller has determined, having regard to the sensitivity of the data, the value of the medium, and the controller's environmental commitments, that physical destruction is the appropriate response.

4.4 Pathway 3: Process-based assurance (Model 3) and why it does not currently discharge the obligation

The framework identifies process-based assurance as the dominant practice in the UK public sector (Section 3.3). This section addresses the position of process-based assurance as a discharge pathway under the fundamental principle established at Section 1.2.

A process-based assurance certificate of the kind currently issued by typical destruction suppliers in the UK public sector does not, by its contents, satisfy the evidential standard at 3.2 and does not carry a warrant of irretrievability that survives reconciliation against the governing licence terms. The certificate records that a process was followed. The governing licence terms typically disclaim responsibility for the outcome of the process, exclude liability for data loss, and cap liability to the licence fee paid. The disclaimer prevails on reconciliation. The warrant the fundamental principle requires is therefore absent.

Process-based assurance is not therefore a discharge pathway in its current form. The DPIA, having reached this finding in Section 3, must identify mitigation under Pathway 1 or Pathway 2. There is no third route.

This finding is not a criticism of the suppliers operating in the sector. Supplier practice has developed over decades against a sector expectation that has not, until recently, required outcome-evidence-based certification supported by an explicit warrant. The suppliers have produced what was specified. The DPIA's finding is that what was specified does not satisfy the accountability obligations under UK GDPR, and that the specification must change.

A controller responding to the DPIA finding may identify with their existing supplier that the supplier is willing to update its certificate format, its licence terms, and its contractual position to bring its practice into Model 1. Where the supplier can do this and the controller can negotiate the contractual changes, the mitigation is achievable within the existing supplier relationship. Where the supplier cannot or will not, the controller's mitigation is a change of supplier or a change to Model 2.

4.5 Downstream warranties and why they do not close the gap

A common response to the finding at 4.4 is that the controller's immediate supplier, typically an ITAD, provides a warranty of destruction to the controller that supplements or replaces the warrant on the certificate produced by the underlying destruction software. The DPIA should consider this position carefully and reach a documented view.

Where the destruction software's licence terms disclaim outcome responsibility, the underlying outcome is not warranted by the party that controls the destruction. An ITAD providing a downstream warranty to the controller is warranting something it does not control. The ITAD does not control the software's internal operation, does not determine which method is applied to which medium, does not enforce correct execution, and cannot prevent unsafe alternatives. The ITAD's warranty is therefore structurally conditional on the software's behaviour, even where the conditionality is not stated explicitly.

If the destruction outcome later proves to be inadequate, because data resurfaces from a medium believed to have been destroyed, the ITAD's warranty will be examined against the underlying software's contractual position. Where the software disclaims the outcome, the ITAD's warranty is contractually unsupported. The ITAD has limited contractual recourse against the software vendor, because of the licence disclaimers, limited operational ability to demonstrate that the outcome was achieved on the specific medium, and limited evidential basis for the warrant it has issued.

The control-and-responsibility alignment principle established at Section 1.2 makes the position categorical. A warrant of permanent destruction must be issued by the party with control of the destruction process. Where the controlling party disclaims the outcome, no downstream party can supply a warrant that closes the gap. The downstream warranty redistributes commercial risk between the controller and the immediate supplier; it does not produce the warrant the fundamental principle requires.

The DPIA should record this analysis where the controller's current arrangements rely on downstream warranties from an ITAD or service provider operating on Model 3 software. The finding is that the downstream warranty does not satisfy the standard at 3.2 and does not constitute mitigation. The mitigation pathways at 4.2 and 4.3 remain the routes by which the obligation can be discharged.

4.6 Certification and accreditation in relation to the warrant

A further response to the finding at 4.4 is that the destruction supplier or destruction software holds independent certification or accreditation, and that this certification validates the outcome. The DPIA should address this position.

Certification and accreditation play a valuable role in establishing supplier and product capability. They demonstrate that the supplier or product has been assessed against defined criteria under defined conditions. They support audit, procurement, and governance processes.

Certification does not, however, supply the warrant the fundamental principle requires. Certification validates capability under defined conditions. It does not warrant the outcome on the specific storage medium in the controller's operational context. The certifying bodies do not accept outcome responsibility, do not warrant irretrievability on specific media, and do not stand behind the destruction result if data later proves recoverable. Their role is to assess conformance, not to underwrite outcomes.

The DPIA should record this where the controller's current arrangements rely on supplier accreditation as the basis for the assurance position. The accreditation may continue to be a valuable input to the procurement process and the supplier management framework. It does not, of itself, discharge the accountability obligations under UK GDPR. The warrant requirement at 3.2 element 8 remains.

4.7 Selection of pathway

The choice between Pathway 1 and Pathway 2 is a matter for the controller, having regard to the controller's circumstances. The factors the controller may weigh include:

1. **Sensitivity of the data.** Higher-sensitivity data may warrant physical destruction regardless of the asset value consequences.
2. **Asset value and environmental considerations.** Controllers with significant equipment refresh volumes may find that evidence-based outcome assurance preserves asset value and reduces environmental cost, where the supplier set supports it.
3. **Operational scale.** Controllers with high-volume destruction operations may find one pathway more practically scalable than the other in their context.
4. **Existing supplier relationships.** Where the existing supplier base supports Pathway 1 capability, the mitigation may be achievable through specification update rather than supplier change.
5. **Sector practice and regulatory expectation.** Some sectors may have developed conventional expectations around pathway selection that should be considered in the controller's assessment.

The framework is supplier-agnostic and pathway-neutral in respect of the choice between Pathway 1 and Pathway 2. Both are valid routes to discharge of the accountability obligations. The framework's only

requirement is that the pathway selected, when implemented, produces evidence and a warrant meeting the standard at 3.2. Neither pathway is given a lighter evidential burden than the other.

4.8 Specification update for procurement

Once the pathway is selected, the DPIA should identify the specification updates required to procurement documentation, supplier contracts, and service level agreements to embed the chosen pathway in the controller's operational arrangements. Specification updates typically include:

1. **Certificate format requirements.** Detailed specification of the fields the destruction certificate must contain, drawing on the requirements at 3.2 and the pathway-specific requirements at 4.2 or 4.3.
2. **Method specification.** Specification of the destruction methodology, by reference to recognised technical standards appropriate to the media types being destroyed.
3. **Verification requirements.** Specification of the verification activity the supplier must conduct on the destruction outcome, and the evidence the verification must produce.
4. **Warrant requirements.** Specification of the explicit warrant the supplier must provide, and the contractual alignment required to ensure the warrant survives reconciliation against the licence terms and service contract.
5. **Reporting and audit rights.** Specification of the supplier's reporting obligations to the controller, the controller's audit rights in respect of the supplier's destruction process, and the controller's right to require independent verification on a sample basis.
6. **Chain of custody documentation.** Specification of the chain of custody documentation the supplier must maintain and provide to the controller.

The DPIA should record the specification updates as an output. The implementation of the specification updates is a matter for the controller's procurement function in coordination with the controller's existing or new supplier relationships, and falls outside the DPIA itself.

4.9 Interim arrangements during transition

Where the DPIA identifies that the controller's current arrangements do not meet the evidential standard and that mitigation will take time to implement, the DPIA should consider whether interim arrangements are appropriate for the destruction of media in the period between the DPIA and the implementation of mitigation. Interim arrangements may include:

1. **Storage of end-of-life media pending implementation of mitigation.** Where storage media reaches end of life during the transition period, secure storage by the controller, pending implementation of the new arrangements, may be appropriate. The controller retains operational control of the media during the storage period.
2. **Use of an alternative pathway during transition.** Where the chosen long-term pathway is Pathway 1 but the supplier transition will take time, the controller may use Pathway 2 on an interim basis, provided the Pathway 2 arrangement itself meets the requirements at 4.3.

3. **Accelerated implementation for high-sensitivity media.** Where particular categories of media carry higher sensitivity, including special category data, criminal conviction data and data relating to vulnerable data subjects, the controller may accelerate implementation of mitigation for those categories ahead of the wider transition.

The DPIA should record any interim arrangements and the rationale for them, and should specify the trigger for transition to the long-term arrangements.

SECTION 5

Consultation

5.1 Consultation requirements under Article 35

Article 35(2) UK GDPR requires the controller to seek the advice of the Data Protection Officer where one has been designated. Article 35(9) provides that, where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

For a DPIA conducted under this framework, the consultation requirements include the DPO consultation under Article 35(2), structured consultation with the internal functions whose operational practice the DPIA addresses, and consultation with the controller's destruction suppliers. Consultation with data subjects under Article 35(9) is considered separately at 5.5.

5.2 DPO consultation

The DPO consultation under Article 35(2) is intrinsic to a DPIA conducted under this framework, on the basis that the DPO is the function leading the DPIA. The framework anticipates that the DPO will be the principal author of the DPIA and that the DPO's advice will be reflected throughout.

Where the controller has appointed a DPO under Article 37 UK GDPR, the DPO should formally record their advice on the DPIA conclusions and the mitigation pathway selected. The advice should address:

1. **The adequacy of the DPIA scope and methodology.** The DPO should confirm that the DPIA properly addresses the processing activity and applies an appropriate methodology.
2. **The conclusions reached.** The DPO should record their view on whether the conclusions of the DPIA are supported by the evidence assessed.
3. **The mitigation pathway selected.** The DPO should record their view on whether the chosen pathway is appropriate to the controller's circumstances and whether the proposed implementation is adequate.

Where the controller has not appointed a DPO under Article 37, because the controller's circumstances do not require designation, the framework anticipates that the equivalent function within the controller, whether Information Governance Manager, Senior Information Risk Owner, or equivalent, will play the same role.

5.3 Internal stakeholder consultation

The DPIA should be informed by consultation with the internal functions whose operational practice it addresses. These typically include:

1. **IT operations.** The function responsible for the day-to-day handling of end-of-life equipment. IT operations holds operational knowledge of the controller's media types, refresh cycles, current supplier arrangements, and chain of custody practice.

2. **Procurement.** The function responsible for the controller's supplier contracts and specifications. Procurement holds knowledge of the contractual frameworks within which the controller's destruction services are obtained, the variation mechanisms available, and the procurement cycles that may affect the timing of mitigation.

3. **Information governance.** The function responsible for the controller's wider information governance framework. Information governance holds knowledge of the controller's record-keeping practice, asset register, and the relationship between the DPIA and other accountability documentation.

4. **Senior Information Risk Owner or equivalent.** The senior officer with accountability for information risk across the controller. The SIRO holds knowledge of the controller's risk appetite, governance structure, and the relationship between the DPIA conclusions and the controller's wider risk position.

5. **Legal function.** The controller's legal advisors, particularly where the DPIA conclusions may have contractual or compliance implications that require legal evaluation. The reconciliation test at 3.2 element 8 specifically benefits from legal input, because the test requires examination of contractual documents alongside operational certificates.

The DPIA should record the consultation conducted with each function, the substantive input received, and the way the input has been reflected.

5.4 Supplier consultation

The DPIA should be informed by consultation with the controller's current destruction suppliers, on the basis that the suppliers hold direct operational knowledge of the processing being assessed. Supplier consultation should focus on:

1. **Specimen certificate analysis.** The supplier should provide specimen certificates for each category of storage media they process for the controller, covering the certificate format actually issued in operational practice. Specimen certificates support the mapping at 3.4.

2. **Licence terms and service contracts.** The supplier should provide the licence terms, end user licence agreement, and service contract that govern their destruction services to the controller. These documents support the reconciliation test at 3.2 element 8.

3. **Methodology disclosure.** The supplier should be invited to disclose the destruction methodologies applied to each media type, and the basis on which the methodology is asserted to be effective on the media type concerned. For physical destruction, this includes the particle size or destruction state produced.

4. **Warrant capability inquiry.** The supplier should be invited to confirm whether they are willing and able to produce certificates that include an explicit warrant of irretrievability supplied by the party with control of the destruction process and surviving reconciliation against the governing terms. The supplier's response informs the assessment finding at 3.5 between Finding B and Finding C.

5. **Upstream supplier position.** Where the controller's immediate supplier is an ITAD operating destruction software supplied by a third-party software vendor, the controller should inquire about the upstream vendor's position on warrant and licence terms. The control-and-responsibility alignment principle at Section 1.2 means that the warrant must be supplied by the party with control. Where control sits with the upstream vendor, the upstream vendor's position is determinative.

The DPIA should record the consultation conducted with each supplier and the responses received. Where a supplier declines to engage with the consultation or declines to provide specimen certificates or licence terms, the DPIA should record the supplier's position and the implications for the controller's assessment of that supplier.

5.5 Data subject consultation

Article 35(9) provides for consultation with data subjects where appropriate. For a DPIA on end-of-life data destruction, formal consultation with data subjects on the destruction process itself is unlikely to be operationally meaningful. The data subjects affected are not in a position to evaluate the technical adequacy of destruction methodologies, and the issue is not one on which their views can practically be sought.

The DPIA should however consider whether the controller's wider data protection notices to data subjects accurately reflect the controller's destruction practice, particularly any commitments the controller has made about how personal data is handled at end of life of the controller's IT equipment. Where the DPIA identifies that current practice does not match the commitments in the controller's notices, the DPIA should record this finding and address the rectification of the notices as part of the mitigation programme.

5.6 Documentation of consultation

The DPIA should record:

1. The functions and external parties consulted.
2. The substance of the consultation conducted with each.
3. The input received.
4. Where input has been reflected in the DPIA, the way it has been reflected.
5. Where input has not been reflected, the reason it has not been reflected.

The consultation record forms part of the controller's accountability documentation.

SECTION 6

Documentation, review and sign-off

6.1 Documentation of the DPIA

The DPIA produced under this framework should be documented as a self-contained record that captures the assessment, the conclusions, and the mitigation programme. The documentation forms part of the controller's accountability documentation under UK GDPR and should be capable of demonstrating, to the Information Commissioner or to any other regulatory or audit function, that the controller has discharged the accountability obligations in respect of end-of-life data destruction. The documentation should include:

1. **Scope of the assessment.** The processing activity assessed, the data categories considered, the data subjects affected, and the operational and temporal scope, drawing on Section 1 of this framework.
2. **Risk identification and assessment.** The risks identified as applicable to the controller's circumstances and their assessment under the controller's own methodology, drawing on Section 2 of this framework.
3. **Assessment findings.** The mapping of the controller's current practice against the evidential standard, the findings for each combination of supplier and media category, and the rationale for each finding, drawing on Section 3 of this framework.
4. **Mitigation pathway selected.** The pathway selected for each combination requiring mitigation, the rationale for the selection, the specification updates required, and the implementation programme, drawing on Section 4 of this framework.
5. **Residual risk and Article 36.** The residual risk recorded after mitigation and, where a high residual risk would remain, the record of consultation with the Information Commissioner under Article 36 UK GDPR.
6. **Consultation record.** The consultation conducted with internal functions, suppliers, and where applicable data subjects, drawing on Section 5 of this framework.
7. **DPO advice.** The formal advice of the DPO under Article 35(2) UK GDPR, recorded in the DPIA.
8. **Sign-off.** The formal sign-off of the DPIA by the controller's appropriate authority, recording the date of sign-off and the authority of the signatory.

The DPIA documentation should be substantive enough to demonstrate the assessment to a third party, whether regulator, auditor or successor DPO, without requiring oral explanation or supplementary briefing. Where the DPIA references external documents, including specimen certificates, licence terms, supplier specifications and technical standards, the references should be specific and the documents should be retrievable.

6.2 Review and reassessment

The DPIA should be subject to ongoing review. Reassessment is triggered by:

1. **Change in operational arrangements.** A change in the controller's destruction suppliers, processes, contracts, or specifications.
2. **Change in media types in use.** Introduction of new media types into the controller's estate that were not assessed in the original DPIA.
3. **Change in regulatory environment.** Material change in the regulatory environment, including formalisation of the regulatory direction indicated by the Cyber Security and Resilience Bill, new ICO guidance, or substantive changes to UK GDPR or its implementing legislation.
4. **Change in supplier capability or supplier-side incident.** A material change in the capability of any of the controller's destruction suppliers, a change to the licence terms or service contract of any supplier, or any incident affecting any of them that calls into question the evidence on which the DPIA relied.
5. **Periodic review.** Routine periodic review at intervals appropriate to the controller's risk profile. A review interval of twelve months is suggested as a default for public sector controllers, with shorter intervals for controllers handling higher volumes or higher sensitivity data.

The DPIA should record the date of the next scheduled review and the trigger conditions that would prompt review before that date.

6.3 Integration with the controller's wider accountability framework

The DPIA on end-of-life data destruction does not stand in isolation. It forms part of the controller's wider accountability documentation under Article 5(2) UK GDPR and interacts with:

1. **The controller's Record of Processing Activities under Article 30.** The end-of-life destruction activity should be reflected in the ROPA, including the suppliers involved and the categories of media processed.
2. **The controller's wider DPIA register.** The DPIA on end-of-life destruction should be recorded in the controller's DPIA register, and cross-referenced from other DPIAs that involve the processing of personal data on physical storage media.
3. **The controller's information asset register.** The storage media subject to destruction should be traceable through the controller's asset register, supporting the chain of custody documentation.
4. **The controller's incident response framework.** Where the DPIA identifies the possibility of historical incidents, meaning storage media disposed of under previous arrangements that may not have met the evidential standard, the controller should consider whether incident response processes are engaged in respect of those historical disposals.

The DPIA should record the integration points with the controller's wider accountability framework and the steps taken to ensure the DPIA conclusions are reflected in those wider arrangements.

6.4 Sign-off and authority

The DPIA should be signed off by an authority appropriate to the controller's governance structure. For most public sector controllers, sign-off is appropriate at the level of the Senior Information Risk Owner, the Caldicott Guardian where applicable, or equivalent senior officer with accountability for information risk.

The sign-off records that the controller has formally accepted the DPIA conclusions, has committed to the mitigation programme, and has authorised the implementation steps required. The signatory's authority should be sufficient to commit the controller to the procurement, contractual and operational changes the DPIA identifies.

The DPO's advice under Article 35(2) UK GDPR should be recorded prior to sign-off, and the sign-off authority should record their consideration of the DPO's advice.

6.5 Status of the completed DPIA

A completed DPIA conducted under this framework documents the controller's accountability position under UK GDPR in respect of end-of-life data destruction. Where the DPIA records that the evidential standard at 3.2 is met across all combinations of supplier and media category, the DPIA documents that the controller has discharged the accountability obligations in respect of the processing activity. Where the DPIA records gaps and a mitigation programme to close them, the completed DPIA and the implementation of the mitigation programme together form the basis on which the controller will discharge the obligations once the mitigation is in place.

The DPIA is not, of itself, a guarantee of compliance. It is the controller's documented assessment of the controller's position and the steps the controller is taking to ensure compliance. The compliance position is achieved by the implementation of the assessment's conclusions.

REFERENCES

Sources and primary references

Every proposition in this framework 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, 9, 10, 24, 28, 30, 32, 35, 36, 37 and 44 to 50.
- Data Protection Act 2018.
- Freedom of Information Act 2000, and Freedom of Information (Scotland) Act 2002.
- 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 framework. Bill 4035, bills.parliament.uk.

Regulatory correspondence and public authority responses

- Information Commissioner's Office, correspondence dated 21 January 2026, case reference IC-471076-R5B2. Cited at Section 1.3.
- Scottish Environment Protection Agency, Freedom of Information response dated 31 March 2026. Cited at Sections 1.2 and 3.3.
- Information Commissioner's Office, published guidance on Data Protection Impact Assessments, including the screening criteria under Article 35 and the prior consultation requirement under Article 36. Cited at Sections 1.3, 1.4, 2.7 and 4.1.

Technical standards and guidance

- NIST Special Publication 800-88 Revision 2, *Guidelines for Media Sanitization*, September 2025. Supersedes Revision 1 of December 2014. Revision 2 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 Sections 2.4, 3.2 and 4.2.
- 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 Sections 2.4 and 3.2.
- 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 Section 4.3.
- National Cyber Security Centre guidance on the secure sanitisation and disposal of storage media, which superseded HMG IA Standard No. 5, *Secure Sanitisation*. Cited at Sections 2.4 and 4.3.

- ISO/IEC 27001, *Information security management systems: requirements*. Referred to at Sections 2.5 and 4.6 as an example of supplier certification.

Where these standards are read together, NIST SP 800-88 Revision 2 sets the sanitization programme, the Clear, Purge and Destroy categories and the validation expectation; IEEE 2883-2022 and IEEE 2883.1-2025 supply the storage and technique-specific requirements and their application; and NSA/CSS Policy Manual 9-12 supplies physical destruction requirements. UK organisations should read NCSC guidance alongside them.

Evidence base

- Freedom of Information programme conducted between January and May 2026. 1,036 requests issued to UK public bodies; 684 substantive responses received; 437 confirmed that no outcome warranty and no device-level evidence is held. Findings as at 22 May 2026. Each response is a public document held by the authority that issued it. Cited at Sections 1.4 and 3.3.

Note on accreditation schemes

Where this framework 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 framework, and no scheme operator has been consulted on or has endorsed its contents.

ANNEX A

Reference material

The following reference materials accompany this framework and may be drawn upon in conducting the DPIA:

1. **Technical reference document on destruction methodologies and evidence requirements.** Detailed technical material on the three assurance models, the technical characteristics of different methodologies, the evidence each produces, and the assessment of methodology adequacy across media types.
2. **Sector evidence summary on current destruction assurance practice.** What a Freedom of Information programme across the UK public sector establishes about current practice, drawn from 684 classified responses given under statutory duty, together with a statement of the scope limits of that programme and of what its evidence does and does not support.
3. **Comparator analysis of specimen destruction certificates.** Side-by-side analysis of specimen destruction certificates representative of the three assurance models, illustrating the evidential characteristics of each.
4. **Sample procurement specification language.** Sample specification language for procurement of destruction services under each of the two valid mitigation pathways at Section 4, for adaptation by the controller's procurement function.

The reference materials are provided as supporting resources to the framework. They do not form part of the framework itself, and their use is not required for the framework to be applied.