Instruction & Confirmation Letter

# Instruction & Confirmation Letter

The current draft of a templated Ministry of Justice (MoJ) data destruction letter, that may be issued by the MoJ to a supplier. The letter describes required actions and information, followed by a responsive declaration from the supplier.

## Letter issued by MoJ

**Background**

For legislative, regulative, privacy and security purposes, it must be possible for Suppliers to decommission and delete (irreversibly 'erase' or 'destroy') data and warrant the same. Similarly, any storage media holding such data must be securely and comprehensively erased before reuse or disposal (such as at end-of-life).

An example of a data destruction obligation is where a Supplier (acting as a 'Data Processor', as defined by Data Protection legislation) working on behalf of, or supplying services to, the Ministry of Justice (the 'Data Controller', as also defined by Data Protection legislation). The Data Processor, including any sub-processor instructed or otherwise involved in Data Processing on the Data Processor's behalf, must comply with instructions from the Data Controller regarding data irrespective of any commercial contract or promise such as a Data Subject exercising the 'right to be forgotten'.

This document provides an acceptable data destruction baseline from the Ministry of Justice, and associated declaration. When followed completely, this baseline for data destruction is considered sufficient to comply with data decommissioning and disposable tasks (and corresponding supplier assurances) for material classified as OFFICIAL under the [UK HMG Government Security Classifications Policy](https://www.gov.uk/government/publications/government-security-classifications) (including sensitive personal data or sensitive commercial data within the same).

**Data Lifecycle**

The Ministry of Justice informally acknowledge that automated systems involved in data management and associated lifecycles may not be capable of immediate decommissioning data on demand. Examples of such systems are data backup and disaster recovery solutions that have a defined and automated data cycle and retention system.

The Ministry of Justice require positive confirmation of the final date by which these systems will have completed their data lifecycle tasks and data destruction will have been completed by.

Where data cannot be erased immediately, there must be methods in place to limit and constrain access to the data until the data lifecycle is complete or manual intervention can be made and subsequent data destruction assured.

The Ministry of Justice reserves all rights regarding instructions relating to data. This includes any need for immediate data destruction.

**Standards**

The following standards and guidelines are the *minimum* basis for data decommissioning or destruction. Follow and apply them as appropriate. There might also be extra steps specific to a data set or system.

* National Cyber Security Centre (NCSC) guidance on end-user device reset procedures: <https://www.ncsc.gov.uk/guidance/end-user-device-guidance-factory-reset-and-reprovisioning>
* NCSC guidance on secure sanitisation of storage media: <https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media>
* NCSC Cloud Security Principle 2: Asset Protection and Resilience (Data Destruction): <https://www.ncsc.gov.uk/guidance/cloud-security-principle-2-asset-protection-and-resilience#sanitisation>
* Payment Card Industry Data Security Standard (PCI-DSS) (Data Destruction): <https://www.pcisecuritystandards.org>
* DIN: <http://www.din-66399.com/index.php/en/securitylevels>

Data Destruction for electronic/magnetic storage **must** include, unless otherwise superseded by NCSC, PCI-DSS or specific MoJ guidance:

* the revocation or otherwise destruction of decryption keys and/or mechanisms to render data inaccessible or otherwise void through the use of modern cryptography; AND/OR
* data overwriting methods consisting of at least 3 (three) complete overwrite passes of random data.

Data Destruction for printed materials **must** include, unless otherwise superseded by NCSC or specific MoJ guidance:

* paper cross-shredding methods to satisfy at least the DIN 66399 Level 4 standard with a maximum cross cut particle surface area 160 (one hundred and sixty) millimeters squared with a maximum strip width of 6 (six) millimeters

The required outcome is to ensure that Ministry of Justice data is inaccessible by any reasonable commercial and resourced means (such as commercially available data recovery services).

## Supplier declaration

*Please sign the declaration below and return this letter to the Ministry of Justice, keeping a copy for your own records. Should you have any queries, please contact the Ministry of Justice CISO via* [*security@digital.justice.gov.uk*](mailto:security@digital.justice.gov.uk)

*Return electronically. Electronic signatures or otherwise positive confirmation are accepted.*

Chief Information Security Officer Ministry of Justice 102 Petty France Westminster, London SW1H 9AJ [security@digital.justice.gov.uk](mailto:security@digital.justice.gov.uk)

Date: \_\_\_\_\_\_\_\_\_\_

We hereby confirm that all Ministry of Justice data, including non-proprietary data generated through the provision of Service, has been suitably, appropriately, and irreversibly destroyed in its entirety and rendered permanently inaccessible and void.

Data backup, including disaster recovery systems, will automatically conduct appropriate data destruction as part of an automated data life cycle on or before the \_\_\_\_\_\_\_\_\_\_ (Strike as applicable)

Anonymised and/or non-Personal Data has been retained for statistical analytical purposes only. We warrant compliance with all applicable data protection and privacy legislation in this regard. (Strike as applicable)

Contract/project reference: \_\_\_\_\_\_\_\_\_\_

For and on behalf of organisation: \_\_\_\_\_\_\_\_\_\_

Name: \_\_\_\_\_\_\_\_\_\_

Position: \_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_