DATA DISPOSAL AND DATA RETENTION

APPROVED BY

PRYSMIAN S.p.A BOARD OF DIRECTORS

April 09, 2025

Code: PO-IT-I&C-SEC015

prysmian

The planet's pathways

TABLE OF CONTENTS

1. PURPOSE & OBJECTIVE

The primary aim of this Policy is to set out limits for the retention of personal/confidential data and to ensure that those limits, as well as further data owner rights to erasure, are complied with. By extension, this Policy aims to ensure that the Company complies fully with any laws obligations and ensuring that excessive amounts of data are not retained by the Company.

In addition, the purpose of this policy is ensuring to dispose confidential data using methods which meet fully the requirements of the Data Protection Law and Security Best practice.

This Policy is based upon the standards set by ISO 27001 series, NIST Cyber Security Framework and the applicable laws and regulations, including – but not limited to – the General Data Protection Regulation (GDPR)

2. POLICY OWNER

Information & Cyber Security Function owns this Policy and is responsible for periodically reviewing and updating it to ensure it accurately reflects organizational updates or legal and regulatory changes.

3. APPLICABILITY

This procedure is intended for all Prysmian Group users, including all employees, contractors, suppliers and visitors that are involved in the retrieval, creation, classification or processing of the confidential Information, each for the specific area of responsibility.

4. YOUR RESPONSIBILITY AS EMPLOYEE

This Policy requires you to:

a) Read, understand, and comply with the requirements included in this Policy;

b) Comply with Prysmian's Code of Ethics and any other applicable policies or procedures.
c) Report immediately to the appropriate channels outlined in Section 6 of the **Helpline Policy** any alleged violation of this Policy, both if committed by a Prysmian employee or an external stakeholder;
d) Ask questions or report any concerns related to this Policy.
e) Complete assigned training related to this Policy when required.

5. GENERAL PRINCIPLES

This policy deals with the retention and disposal of confidential data stored in Prysmian Group. It is necessary to have a policy to ensure that accurate and complete records of all business activities are created, captured, maintained and destroyed in a consistent, systematic, secure and reliable manner and in accordance with legal, regulatory, operational and historical requirements.

Failure to manage records can result in very serious consequences for the Group including enforcement actions by the regulators, an inability to defend or pursue litigation, and material impact to the operation of the business, leading to reputational damage.
In Prysmian Group's confidential records are usually based on electronic format but may take other forms. It is important that the correct method of disposal is used both regarding the medium on which the record is stored and the type of personal information that is being destroyed.

Records received from external parties are subject to the requirements set out in this Group Policy Standard. They must be managed in the same way as those records created in the conduct of Group business.

6. ROLES & RESPONSIBILITIES

The following table describes the roles involved in the data Disposal and Data retention process and their responsibilities:

Role	Responsibilities
Information Owner	• To destroy information in line with the retention period • To destroy personal information on data subject request • To verify, before data destruction, if there are legal or Judicial pending process. • To define the data retention period for personal data
Legal	• Inform information owner about legal/judicial process on data
ICT Personnel	• Apply the data destruction methods according this policy • Support Information Owner on secure data destruction
Security Personnel	• Provide guidance on secure data destruction and tool
DPO	• The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy.

	• The Data Protection Officer shall provide guidance and conduct monitoring activities on compliance with the identified data retention periods throughout the Company. • Provide support in identifying the data retention period for personal data

Table 1: Roles and responsibilities

7. HOW LONG WE SHOULD KEEP RECORDS.

Before identifying the correct record retention period, it is necessary to classify the information, according to the Data Classification Policy.

We need to assess records to:

- Determine their value as a source of information, its operations, relationships and environment
- Assess their importance as evidence of business activities and decisions
- Establish whether there are any legal or regulatory retention requirements

The retention periods can differ based on the type of data processed, the purpose of processing or other factors.
It is important identify the type of data to keep as below:

- Legal: documents and data that must be kept for a specific period of time as required by local laws or provided by multinational organizations (such as the European Union)
- Business: data, documents and information that may be useful for the company for future projects and activities or which must be kept for a certain period of time defined by law (for example information on contracts, proposals or projects).

- Other: data that does not have a specific retention period or that must be stored according to regulations

8. THIRD PARTY

You must not delegate responsibility for disposal of personal information to a third party except in the following cases:

- Group making use of a formal written agreement with an external party for the disposal of data.
- There may be occasions when there are 3rd parties processing data on our behalf. Upon termination of the contract or agreement with the 3rd party, the Group needs to ensure that those 3rd party suppliers dispose the personal data they hold on your behalf appropriately and securely. There should be reference to how the 3rd party will dispose of the personal data within the contract or agreement the Prysmian has signed. It is imperative that this is checked upon termination.

9. UNDERSTANDING WHEN DATA MUST NOT BE DESTROYED

Data whether classified Confidential or Confidential Restricted, must not be destroyed if they are Historical (permanently preserved by the Group for historical reasons because they document key strategies, policies, decisions, activities, people, properties, products or services.) or are subject to litigation, regulatory enquiries or audit activities are taking place or are about to take place, even if the retention period has passed.

10. DATA RETENTION

Different types of data, used for different purposes, will necessarily be retained for different periods (and its retention periodically reviewed), as set out in the table of retention period (appendix A).

10.1 When establishing and/or reviewing retention periods, the following shall be considered:

a. The objectives and requirements of the Company.
b. The type of data in question.
c. The purpose(s) for which the data in question is collected, held, and processed.
d. The Company's legal basis for collecting, holding, and processing that data.
e. The level of classification of data and to whom the data relates.

10.2 If a precise retention period cannot be fixed for a particular type of data, criteria shall be established by which the retention of the data will be determined, thereby ensuring that the data in question, and the retention of that data, can be regularly reviewed against those criteria.

10.3 Notwithstanding the defined retention periods, certain data may be deleted or otherwise disposed of prior to the expiry of its defined retention period where a decision is made within the Company to do so.

10.4 In Limited circumstances, it may also be necessary to retain personal data for longer periods where such retention is, for archiving purposes, legal purpose, or historical business purposes. All such retention will be subject to the implementation of appropriate technical and organizational measures to protect the rights and freedoms of data subjects, as required by the GDPR.

11. DURING THE RETENTION PERIOD

The following rules must be applied:

- Establish periodical reviews of data retained.
- Establish and verify retention periods for data considering the following categories:
  a. the requirements of your business.
  b. type of data and classification.
  c. purpose of processing.
  d. lawful grounds for processing.

- If precise retention periods cannot be established, identify criteria by which the period can be determined.
- Establish periodical reviews of data retained.

12. SHARING OF CONFIDENTIAL INFORMATION

Duplicate records should be destroyed. Where information has been regularly shared between business areas, only the original records should be retained.

Where we share information with other bodies, we will ensure that they have adequate procedures for records to ensure that the information is managed in accordance with the Authority's policies, relevant legislation and regulatory guidance.

13. DISPOSAL

Information can be disposed when no longer necessary for the purposes for which the data is processed or when required by law.
The Information Owner has to ensure its proper disposal and, if necessary, its destruction, together with any further produced copies. Adopted disposal modalities must be adequate to the Information classification level.
Destruction of electronic records should render them non-recoverable even using forensic data recovery techniques.

Upon the expiry of the data retention periods set out below in Annex1 of this Policy, or when a data owner decides to have their data erased, data shall be deleted, destroyed, or otherwise disposed of as follows:

- Data stored electronically (including any and all backups thereof) shall be deleted securely.
- Special category data stored electronically (including any and all backups thereof) shall be deleted securely.

- Data stored in hardcopy form shall be shredded.
- Special category data stored in hardcopy form shall be shredded.

If is not possible to completely erase the personal data, it is sufficient to anonymize it. This may, for example, be achieved by means of:

- erasure of the unique identifiers which allow the allocation of a data set to a unique person.
- erasure of single pieces of information that identify the data subject (whether alone or in combination with other pieces of information).
- aggregation of personal data in a way that no allocation to any individual is possible.

In some cases, no action will be required if data cannot be allocated to an identifiable person at the end of the retention period, for example, because:

- the identifying data has already been deleted.

14. APPROVED DATA DESTRUCTION METHODS

Four Data Destruction methods are acceptable for use in Prysmian Group. These methods must be implemented by IT Service Providers and third-party suppliers:

- Overwrite
- Secure Erase
- Degauss
- Physical Destruction

See Appendix C for approved methods.

15. STEPS FOR DATA DISPOSAL

1. Check that the proposed disposal of data is in line with department's data retention guidelines, this will differ greatly depending on the type of information involved.

2. Ensure that there are no relevant proceedings in progress relating to individuals identified in the data: for instance, internal disciplinary action, contract disputes or legal authority's actions.

3. Get formal approval from data owner, so data can be destroyed.

4. Identify and use the appropriate means of disposal below:

- Records stored on a Desktop, Laptop or similar electronic device (where the device is to be re-used)
  If the relevant records form only a part of a database, spreadsheet or similar file, then removal of those records using the internal erasure procedure of the relevant program is acceptable
- Records stored on a Desktop, Laptop or similar electronic device (where the device is not expected to be re-used)
  Where the device storage is not to be used in the future, physical destruction of the device must be performed.
- Network based computer records
  The standard file deletion routines are sufficient for network-based files.
- Cloud based records
  The standard file deletion routines are sufficient for cloud-based files.
- Emails
  The emails that contain sensitive personal data must be done using a certified and verifiable instrument, in order to prove the execution of the process.
- Paper
  The minimum standard for the destruction of paper containing personal information should be shredding using shredding machines.
- Paper stored outside the company:

For paper stored outside the company in a third-party storage, if the paper to dispose, are stored in the same box, the supplier can destroy the entire box according to standard requirements as Appendix E and provide a destruction certificate.
If paper (single paper, booklet, dossier, dox) are stored in a box with other documents, the information owner must recall the box, extract the paper expired and destroy it following the standard rules for paper.

- External Hard Disk
  Where they are to be reused may be overwritten and erased with special tool, or subjected to degaussing when are to be dismissed.
- Memory Sticks, Tablet, Mobile Phone memory and similar
  Methods of disposal of records will vary by device type for memory sticks, tablets etc.
  Data owner is responsible to apply a secure deletion to the devices or ask IT Services to perform permanent erasure.

16. CONSEQUENCES OF POLICY VIOLATION

As a Prysmian employee, you are agreeing to uphold our commitment to this Policy. Prysmian employees who violate this commitment or do not comply with this Policy shall be subject to disciplinary procedures, including possible dismissal, and any other legal action required to protect the interest and reputation of Prysmian, in line with the applicable legislation.

17. REPORTING A POLICY VIOLATION

All employees, contractors, and third-party users are required to report any suspected or actual violations of this Information Security Policy or any Security Incident immediately. All reports will be treated confidentially and investigated promptly. Ensuring the integrity and security of our information systems is a collective responsibility, and your cooperation is essential in maintaining a secure environment.

It is critical that potential violations are reported, internally, promptly as this may allow for

immediate containment of any situation and prevention of an actual breach. Additionally, reporting is required to allow Prysmian to take the appropriate action, internally and externally, with regulatory reporting if it is required. Communication with the regulatory authority will be managed and coordinated by Corporate Affairs to protect the reputation and manage the liabilities of Prysmian.

As a Prysmian employee, you are required to report any Policy violation to:

a. **Cybersecurity@prysmian.com;** or
b. your Regional Compliance Team or the other designated subjects mentioned in Section 6.1 of the **Helpline Policy**.

Any form of retaliation, including threats and attempts of retaliation, is strictly prohibited. Prysmian is committed to ensuring that all employees are free to disclose any violation, either real or suspected, of the Prysmian's Company policy or procedure, to the extent they have reasonable grounds to believe that the matters reported are true. You will not be adversely impacted or retaliated upon in the workplace, either personally or professionally, for raising a valid and legitimate concern.

18. AUDIT, MONITORING AND CONTINUOUS IMPROVEMENT

The Owner of this Policy is responsible to perform periodic reviews and updates of this document, examining, in particular, revisions to be made based on internal organizational updates, changes to external legislation and best practices.

Using a risk-based approach, on a periodical basis the Information Security Function and the Internal Audit Department may perform, respectively, monitoring or audit activities aimed at verifying the correct enforcement of this Policy within the organization.

19. RELATED DOCUMENTS

The following Documents are related to this Policy and must be consulted by all Prysmian employees for further guidance. Part of such documents are available in the Ethics & Integrity Section of our **Company's Intranet** and are also publicly available within the correspondent Section of our **Corporate website.**

1. "Document and Record Management"
2. "Information Security Policy"
3. "Data Classification Policy"
4. "Data protection Policy"

APPENDIX A – DOCUMENT HISTORY

The history of changes is shown below. The most recent changes are listed first.

Version	Date	Major Changes
1	01/30/2020	First release
1.1	07/11/2022	Revision and Update
1.2	09/04/2025	Change template and Revision

APPENDIX B – DATA RETENTION SCHEDULE

Document	Annex
Retention table	SharePoint link

APPENDIX C - DATA DESTRUCTION METHODS FOR DEVICES

The method of Data Erasure chosen should be based on requirements, which should consider:

- The type of storage device (see Table 1).
- If the device is to be re-used, or decommissioned.
- The data stored and its classification (e.g. Personal data, Credit Card data, classification label of Confidential Restricted');

- Whether the data is protected in any way (e.g. Encrypted, anonymized, obfuscated); and
- Whether the device is owned by Prysmian Group or another party.

Multiple destruction methods may be used on the same storage device to provide a higher degree of assurance that the data is not retrievable. If the storage media contains Confidential Restricted data that is not encrypted, an Overwrite, Secure Erase or Degauss must be conducted prior to a device leaving Prysmian premises for transport to a supplier's site for Physical Destruction.

- Storage devices to be Re-used
  - Use Overwrite or Secure Erase (ATA hard disks only) method.
  - Degauss can also be used on Magnetic Tapes and Floppy Disks, but not on Hard Disks which are destroyed by Degaussing.
- Storage devices to be Decommissioned
  - Use any of the four Data Destruction methods depending on the type of media (please see Table 1).
  - If Physical Destruction is chosen for a storage device that contains unencrypted data classified as Secret and transport will be required to a third-party site, then Overwrite, Secure Erase or Degaussing must be used in addition prior to transport.
- Sale of IT Equipment

  In case of selling data storage devices or returning devices to a supplier under warranty or under a lease agreement, data storage devices must be treated as follows:
  - Data must be destroyed using the Overwrite, Secure Erase or Degauss methods following the requirements documented in 'Details of the Data Destruction Methods' (see Table 1); and
  - All storage devices must be tested to confirm that all Prysmian data has been successfully destroyed or erased.
- Failed Storage Devices

  Storage devices that have failed and are not readable must be treated as follows:

- Devices that are not repaired must be destroyed using Degauss or Physical Destruction methods following the requirements documented in 'Details of the Data Destruction Methods' (see Table 1); and
- Devices that are repaired and are not returned to Prysmian for re-use must have all data destroyed using the Overwrite or Secure Erase methods following the requirements documented in 'Details of the Data Destruction Methods' (see Table 1).

APPENDIX D – APPROVED OVERWRITING STANDARDS

One of the following erase standards must be used.

Infosec Standard 5 (Higher Overwriting Standard)

In this standard, three overwriting circles are used as well as a full verify.
Overwriting of all blocks with the pattern 0x55.
Overwriting of all blocks with the pattern 0xAA.
Overwriting of all blocks with a random pattern.
Full verify.

The standard accepts up to (and including) 50 bad blocks on the media (bad blocks are sections of magnetic storage media that cannot be reliably used for storing and retrieving data). The physical address of the bad block is written to the erase report. The erase process terminates if more than 50 bad blocks is being reported.

US DoD 5220.22M

In this standard, three overwriting circles are used as well as a full verify.
Overwriting of all blocks with the pattern 0x01.
Overwriting of all blocks with the pattern 0xFF.
Overwriting of all blocks with a random pattern.
Full verify.

US NIST Standard SP800-36 & SP800-53

In this standard, three overwriting circles are used as well as one quick verify. Full verify can be enabled.

Overwriting of all blocks with a random pattern.

Overwriting of all blocks with the pattern 0x55.

Overwriting of all blocks with the pattern 0xAA.

Quick verify.

APPENDIX E – DATA DESTRUCTION REQUIREMENTS FOR DIFFERENT TYPES OF STORAGE

A tick (√) in the table below indicates if a particular destruction method can be used with a particular type of storage device.

Totally new types of storage device may require a new assessment to be made, and an addition or amendment to this table. The latest version of this document must be used.

	Overwrite	Secure Erase (ATA Hard Disks only)	Degauss	Physical Destruction
Strorage Type	DIGITAL			
Hard Disk (ATA)	√	√	√	√
Hard Disk (SCSI)	√		√	√
Magnetic Tapes	√		√	√
Others magnetic disks	√		√	√
Smart Cards	√			√
CDs and DVDs				√
USB Memory Devices	√			√
Memory Cards & Sticks (micro SD, mini SD, Compact Flash, XD, MMC etc.)	√			√

Mobile phones, Tablet, Mobile devises, PDA	Manually delete all information, then perform a manufacturer's hard reset to erase all data and reset the device to its factory state. Follow the manufacturer's full sanitization procedure.			√
Storage Type	PAPER			
Single sheets / Booklets / Dox				√
Notebook / Hardcover book				√

APPENDIX F – PAPER DESTRUCTION REQUIREMENTS

Type of paper	Type of paper cut	Minimal size after shredding	Example
Confidential paper	**Cross-cut** – Medium level of security	<320 mm² < 2 mm	
Confidential restricted paper	**Micro-cut** – High level of security	< 30 mm² < 2 mm	