Privacy Organization model

APPROVED BY PRYSMIAN S.p.A BOARD

OF DIRECTORS ON MAY 7th, 2025

The planet's pathways

TABLE OF CONTENT

1. PURPOSE & OBJECTIVE

The purpose of this policy is to describe the main privacy and data protection roles within Prysmian Group (hereinafter, "Prysmian" or the "Group") and provide their tasks and responsibilities according to current legislation on the protection of personal data, with specific reference to Regulation (EU) 2016/679 (Regulation on data protection, hereinafter "GDPR" or "Regulation"), and guidelines on the actions to be taken and the procedures to be carried out to ensure coordination between the Data Protection Officer (or "DPO") appointed by Prysmian and the local contact point of each of the Companies (hereinafter, the "Company").

2. POLICY OWNER

The DPO 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 Policy applies to all employees, interns, external consultants, officers, directors and administrators of all legal entities of Prysmian that fall within the scope of application of the GDPR (Article 3 GDPR). Prysmian Group must evaluate any exemptions from compliance with particular provisions of this Policy.
Exemptions will only be considered if:

- Any particular circumstances do not allow the implementation of a requirement (e.g., compromise of ongoing investigations by other Authorities).
- A local law or regulation providing an exception.
- Compensatory controls mitigating risk

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;

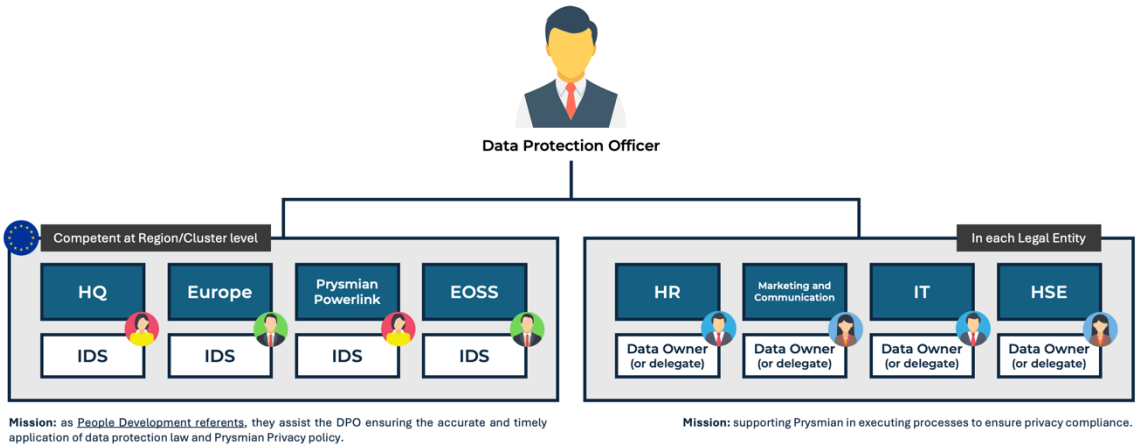
d) Ask questions or report any concerns related to this Policy;

e) Complete assigned training related to this Policy when required.

5. POLICY REQUIREMENTS – ROLES

The main privacy and data protection roles that are identified and assigned are:

- DPO: the person designated by the Controller or Processor to monitor compliance with the GDPR, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits to the Data Subjects, for matters connected to the processing of personal data. In Prysmian, the role of the DPO is different, depending on whether the role is acted by the DPO formally appointed in a Country or by the DPO who operates at Group level in accordance with the Privacy Organizational Model. Here below the DPO tasks are listed, as provided within the GDPR, valid for the countries where he/she is locally appointed, and then the description of the tasks performed by the Group DPO
- Internal Data Supervisor: the person responsible for assisting the local management in adopting, implementing and managing, at Region/Cluster level, standards, policies, procedures and processes, in line with those established by group DPO.
- Data Owner: the head of an area/department that processes personal data, who can delegate the fulfilling of privacy tasks to one or more member of his/her team. Despite the opportunity to delegate, the Data Owner remains totally accountable for the tasks and responsibilities assigned to him/her into the policy.



The instructions provided in this document have been prepared according to:

- the decisions adopted by the local Authorities responsible for the protection of personal data (hereinafter, the "Authority" or "DPA");
- the best practices of the sector that have been developed over the years;
- the Guidelines on Data Protection Officers (WP243), adopted by the Article 29 Working Party (hereinafter, "WP29") on 5 April 2017 (hereinafter, the "Guidelines").

5.1 DPO role according to the GDPR

This paragraph explains the main characteristics of the DPO role, as provided by the GDPR. It applies only to the legal entities of the Group in which the DPO is formally appointed. In such regard, the DPO is responsible for the following activities:

- advising the company on its obligations under the legislation on the protection of personal data,
- monitoring (and ensuring) legal compliance,
- acting as a point of contact for the competent Supervisory Authorities, i.e., the local/main authorities responsible for the protection of personal data (hereinafter, the "Authorities" or "DPA").

The DPO must be appointed considering his/her professional qualities, in particular on the basis of the deep knowledge of data protection law and practice, and the ability to carry out the tasks entrusted to him/her efficiently.

Expert knowledge must be established based on the types of processing implemented at company level, particularly in consideration of the sensitivity, complexity and quantity of data undergoing processing.

Required skills include:

- extensive knowledge of national and European laws and practices on data protection and data security.
- awareness of the processing operations carried out by various corporate functions.
- expertise in information technology and security measures.
- specific knowledge of the market sector in which the company operates and of its internal organization.
- ability to promote the culture of data protection at company level, contributing to the implementation of the key elements of the Regulation, such as the fundamental

principles of processing, the rights of data subjects, privacy-by-design and privacy-by-default criteria, the preparation of adequate records of processing activities, the adoption of appropriate security measures for the management of the identified risks and the correct management of any personal data breaches

5.1.1 DPO responsibilities

The following tasks must be performed by the DPOs appointed pursuant to the GDPR even if the extent of the tasks assigned to the latter is left to the discretion of the data controller (or processor), also in consideration of the sensitivity, complexity and quantity of the personal data involved. In any case, by means of an appointment or equivalent resolution of the competent corporate bodies, it must be ensured that the DPO performs at least the following responsibilities:

Area	Responsibility	Frequency	Evidences	References
1. Policies, procedures and templates	• Publication and updating of policies, procedures and any other necessary documentation or templates (e.g., letters of appointment to System Administrators, instructions to people in charge of processing). • Adequate communication of such documentation within the company (e.g., publication on the intranet).	On event	Set of approved policies	Set of approved policies
2. Data Owner	• Define the document to assign the responsibilities to the Data Owner.	When the responsibilities of the Data Owner will change	Email to the Data owner	Privacy organization model policy

3. Instructions to persons in charge of processing	• Define and update the template of instructions to person in charge of processing. • Communicate these instructions appropriately within the company (e.g., posting on the intranet).	Annual (if needed)	Template of instructions to person in charge of processing	Privacy organization model policy
4. System Administrator	• Define and update the System Administrator appointment template and share it with Information & IT security. • Verify the identification and appointment of System Administrators by Information & IT security. • Where necessary, support Information & IT security in the process of customizing the appointment template, considering systems for which the System Administrator is responsible, and the personal data processed through it.	• If needed (regarding update of the template to appoint System Administrators) • Annual (verification on appointment of System administrators)	System Administrator Appointment Template	Privacy organization model policy
5. Training & awareness	• Provide specific training to all functions within the Company, preparation and updating of training materials on privacy and data protection.	On event	GDPR training materials	Privacy organization model policy

	• Plan and deliver the training sessions.			
6. Record of processing activities	• Ensure periodic updating of processing records (both as Controller and Processor, when applicable).	• Upon need (e.g. in all cases when a processing in place is substantially modified, or a new processing activity is undertaken); • At least annually	• Record of processing as Data Controller • Record of processing as Data Processor	Record of processing activities
7. Privacy notices and consents	• Map all channels of personal data collection, e.g., websites, product sheets or information files. • For each identified channel, prepare the appropriate privacy notices and consent form, when required. • Update of all privacy notices and consent forms. • Verify the proper acquisition and management of required consents.	• In case a new data collection channel/method is implemented; • Annual (if needed)	• Mapping of the channels of personal data collection; • Privacy notices; Consents forms.	Privacy organization model policy
8. Data subject rights	• Analyse and respond to data subjects' requests with the cooperation of Data Owner. • Maintain an up-to-date list of requests on privacy rights.	Whenever a data subject request is received	• List of requests to exercise privacy rights received by the Company.	Data Subject rights policy

			• Correspondence with data subjects	
9. Extra-EU personal data transfers	• Map the extra-EU personal data transfers. • Verify that personal data transfers outside the European Economic Area are carried out in accordance with applicable requirements. • Perform periodic Data Transfer Impact Assessment.	• In all cases when a new data processing is undertaken which implies an extra-EU data transfer; • Annual (if needed)	• Mapping non-EU personal data transfers • Data Transfer Impact Assessment	Transfer of personal data
10. Privacy by design & by default	• Maintain an up-to-date list of privacy screenings performed by Data Owners. • Verify on the timely completion of privacy screenings by Data Owners. • Evaluate the privacy screenings received.	Whenever a new project or process involving the processing of personal data is being planned	• Privacy screening sheet • Updated list of privacy screenings	Data Protection by design and DPIA policy
11. Data Protection Impact Assessment	• Support Prysmian's competent functions in performing Data Protection Impact assessments on the Processing of Personal Data. • Monitor the execution of the Action plan, if it is defined in the DPIA.	Whenever a Privacy screening requires to perform a DPIA	• DPIA • Updated list of DPIAs performed	Data Protection by Design & DPIA policy

	• Maintain an up-to-date list of DPIAs performed.			
12. Data breaches	• Assess the data breach events. • Maintain an up-to-date list of potential and actual data breach events and their supporting assessments.	Whenever an event occurs	• Potential and actual data breach assessment • Updated list of potential and actual data breaches	Data breach incident management procedure
13. Data retention	• Assess the suitability of retention periods identified by Data Owners. • Verify that a structured process is in place to ensure the deletion (or anonymization) of personal data once the identified retention period has ended.	• In all areas when a new data processing is undertaken, for which an appropriate data retention period must be identified; • Annual	Identification of data retention period	Data Retention Policy
14. Security measures	• Check on the implementation of appropriate technical and organizational security measures to adequately protect personal data.	Annual	Baseline security measures	Privacy Organization Model policy

15. Data processors	• Help Data Owners verify that external service providers/outsourcers to be appointed as Data Processors offer adequate guarantees that they will put in place suitable technical and organisational measures so that the processing complies with the GDPR and protects the rights of individuals. • Make the template for designation as data processor available to Data Owner. • When necessary, support the contract owners in the process of appointing suppliers as Data Processors whenever they process personal data on behalf of the Company. Particularly, the DPO gives support in adapting the Data processing agreement to the specific service provided and to the characteristic of the data processing. • Maintain an updated list of appointed data processors. • Maintain an up-to-date file containing copies of Data Processing Agreement	Continuous activity	• Data Processing Agreement template • Repository of signed Data processing agreements • Updated list of the Data Processors • Audit plan • Checklist of audit on Data processors • Audit reports	Privacy Organization Model policy and Vendor Management (procedure)

	• Establishment and execution of an annual audit plan on the most relevant Data Processors.			
16. Second level checks	Perform second-level checks on Data Owners to verify the following areas: • Records of processing activities; • Privacy notices e consents; • Extra-UE data transfers; • Privacy by design & by default; • Data retention; • Security measures; • Data Processors.	Annual	• Checklist of second level checks • Report	Privacy Organization Model policy
17. Relation with the Authority	• Communication to the Data Protection Authority and eventual documents' sharing in case of audit carried out by Authority, or prior consultation according to Art. 36 GDPR.	Whenever the communication is sent/received.	Copy of the communication	Privacy Organization Model policy
18. Reporting	• Preparation of the annual report to the Board of Directors or Risks and Control Committee.	Annual	Report DPO	• Privacy Organization Model • Monitoring and reporting

During its supervisory activities, the DPO must conduct a careful analysis of the risks relating to the processing, taking into account the nature, scope, context and purposes of the processing. In particular, the DPO is required to establish an order of priorities in the exercise of his/her supervisory functions, focusing more on issues which, based on his/her prudent assessment, could imply greater risks in terms of data protection.

5.1.2 Internal and External DPO

The person designated to perform the role of DPO, also through the creation of a dedicated office and team, can be appointed within or outside the organization of the data controller and data processor.

- Internal DPO: If the DPO is chosen among people with whom the company maintains employment relationships, it is essential that the selected person does not hold positions, especially managerial ones, which could give rise to conflicts of interest. Therefore, the internal DPO cannot simultaneously fulfil the role of DPO and head of a company function that establishes the purposes and means of data processing.
- External DPO: The role of DPO can also be performed based on a service contract stipulated with a natural or legal person outside the company of the data controller. Also in this case, in choosing the person to be appointed, all the subjective and objective requirements provided by current legislation must be met, as further specified in this policy and in the WP29's (now EDPB's) Guidelines.

5.1.3 DPO contact

The contact details of the DPO, such as the postal address and a specific email address, must be:

- included in all Information Notices provided to the data subjects, pursuant to art. 13 and 14 of the GDPR;
- published in such a way that the Authority, or other supervisory authorities, can easily contact the DPO;
- communicated to the Authority and, according to good practices, also to all employees (for example, via the company intranet) and to third party managers

5.1.4 Guarantees for DPO office

To enable the DPO to fulfil his/her duties autonomously, with independence and in accordance with current legislation, the Data Controller must provide the DPO with all the resources (e.g. financial, staff, knowledge and continuous training) necessary for the

adequate, efficient and timely execution of such duties. This requirement is met if the DPO can have:

- active assistance from senior management (for example, the Board of Directors).
- sufficient time to carry out the duties for which he/she is responsible (in particular, to prevent the activities entrusted to the DPO from ending up being neglected due to conflicts with other company priorities).
- adequate support in terms of financial resources, infrastructure (office, equipment, tools) and, if appropriate, internal staff and external consultants.
- official communication to all Prysmian's personnel of the appointment of the DPO, to ensure that the presence and functions of the DPO are well known within the company.
- guaranteed access to other services (human resources, legal department, IT, security, etc.) to be able to receive all the assistance and essential information.
- continuous training, to stay constantly updated on developments in the data protection sector and gradually increase his/her level of skills.
- creation of a DPO office or working group (comprising the DPO and suitable support staff), where necessary or appropriate in view of the size and structure of the company. In these cases, it is advisable to precisely define the internal structure of the working group, as well as the individual tasks and responsibilities.
- without any instruction from the appointing data controller (or processor) regarding the performance of his/her duties, without any interference from other company functions, including top management.
- knowing that he/she cannot be sanctioned in any way (or threatened) or removed from office in relation to the exercise of his/her duties.
- with the guarantee of reporting directly to the governing bodies (e.g., CEO or Board of Directors). It is possible that the role of DPO is entrusted to a person who already performs tasks other than those typical of that position (for example, Chief Compliance Officer); in this case, it is essential to organize the corporate governance structure in such a way that this person, in his capacity as DPO, can report directly to the top management of the data controller (or processor), even if this condition is not foreseen for the other office that the person holds.

5.1.5 DPO Engagement

It is essential that the Data Protection Officer, and his/her eventual team, are involved as soon as possible in any matter relating to the processing of personal data.
Furthermore, in consideration of the need for a direct dialogue with the top management, it is necessary that the DPO is punctually invited to take part in the working groups which from time-to-time deal with the processing activities. To this end, it should be ensured:

- that the DPO can regularly join management meetings where issues that could have an impact on data security and the rights of data subjects are discussed.
- that the DPO has all the information necessary to be able to provide adequate advice in a timely manner whenever decisions regarding data processing have to be taken.
- that the opinion of the DPO is always duly taken into consideration and that the reasons supporting the decision taken by the company are documented when the decision is supported by the DPO.
- that the DPO is immediately consulted whenever a data breach or any other relevant event occurs, or when the occurrence of a data breach or event is suspected

5.2 Group DPO

For the other Group companies where the DPO is not formally appointed, Prysmian's DPO ensures and monitors privacy compliance by verifying that each Company's policies, procedures and documents comply with all Group's standards and that they are consistent with the corresponding document in each legal entity of the Group.
During the above-mentioned activities, the Group DPO is responsible for monitoring and coordinating the activities of the following privacy roles to ensure privacy compliance at group level:

- Internal Data Supervisor at European level.
- Privacy Focal Point, who may correspond to an Officer operating within the following Department, depending on the organization of the Company concerned:
  - Compliance,
  - Legal,
  - Information Technology,
  - Security

5.3 Internal data supervisor

The Internal Data Supervisors ("IDS") represent a role appointed by the appropriate local executive or committee, in agreement with the GDPR. Evaluation criteria for the designation depend also on country's internal business, departments, region, and subsidiary company structure and complexity of the organization.

IDS is responsible for assisting the local management in setting the appropriate "tone at the top" of their business organization in order to comply with the Group's and local privacy requirements. IDS implements and manages the Global Privacy Program at a local level by maintaining day-to-day compliance procedures and controls.

He/she is responsible to monitor, in accordance with the law, that the data processing associated with the activities carried out by his/her department, and any other activities that the Data Controller may decide to entrust to him/her in the future, are carried out in full compliance with the applicable legislation, including the relevant provisions issued by the competent Data Protection Authorities.

The complete list of personal data processing activities delegated to his/her area of responsibility is set out in the Record of Processing activities that has been prepared and is updated periodically by the Data Controller.

In particular:

Task	Description
1. Record of processing activities management	• The IDS must: o Help the relevant corporate department in the regular maintenance of the Record of Processing activities. To this end, he/she shall transmit to that department all the information related to the processing of personal data carried out within the Department for which he/she is responsible, as well as any changes regarding the processing and the means by which they are carried out, and any third parties involved. o Ensure that such data is essential and relevant to carry out the specific purposes of his/her area of responsibility. If these principles (essential nature and

	relevance of the data) are not met, he/she has to stop processing after consulting the Data Protection Officer.
2. Special categories of personal data	Whenever the processing of such personal data is necessary, the IDS must contact the DPO and possibly the IT department to determine the most appropriate processing methods.
Legal obligations	• The IDS must ensure that all data processing activities falling within his/her area of responsibility are carried out in compliance with legal obligations. In particular, with regard to data subjects, he/she must ensure the fulfilment of obligations related to: o provision of relevant Information, o request for consent, when necessary, o existence of an adequate legal basis for the processing, o exercise of the rights guaranteed to data subjects, particularly when the processing concerns sensitive data or data relating to minors. • In the event new requirements for processing arise or potential conditions for inadequate compliance with legal provisions emerge, he/she has the responsibility to promptly consult the Data Owners and the DPO to determine appropriate corrective actions to be taken, including the performance of a Data Protection Impact Assessment, in accordance with the relevant policy adopted by the Company
Technical and organizational security measures	The IDS must verify that personal data processed within his/her area of responsibility are kept secure and controlled in such a way as to minimize the risk of destruction or loss, including accidental or unauthorized access, or unauthorized processing or processing not in accordance with the purpose of data collection.

	He/she will also need to verify that appropriate measures are implemented for the security of the processing.

Person in charge of processing	• The IDS must:
	  o coordinate the activities of personnel (employees, interns, consultants, etc.) who carry out the processing of personal data in his/her area of responsibility and verify that they have been duly authorized to carry out the relevant data processing operations and that they receive the necessary instructions on the obligations to be fulfilled in the performance of the tasks assigned to them.
	  o monitor the timely compliance with the instructions that the Data Controller has provided to the employees who have access to personal data or who are involved in their processing.
	• When required, in agreement with the DPO, he/she may establish diversified instructions to be provided to the person in charge of processing according to the operational areas within his/her area of responsibility and the activities specific tasks assigned to them.
	• He/she shall promptly inform the DPO if becoming aware that one or more persons in charge of processing, even if not operating under its responsibility, have violated the obligation of secrecy, or have committed serious actions or violations that may in any way compromise the security of the data or databases.

Training and Awareness	The IDS must monitor compliance with internal procedures and instructions and must contribute to ensure the awareness on the topics provided in the training plan. He/she has the responsibility to increase the attention of his/her colleagues in relation to the protection of personal data and, more generally, in the proper

	management of the company data in order to reduce and minimize risks.
Application of privacy-by-design and by-default principles	In order to ensure that the processing of personal data is carried out in accordance with the principles and legal requirements established in the applicable data protection legislation, the IDS must ensure that all Data Processors operating under its responsibility operate according to the principles of privacy by design and privacy by default. The same obligation must be fulfilled also regarding the protection of data subjects' rights when innovating business processes and defining and launching new products and services, by including this assessment as structural step in the process itself. In assessing these aspects, he/she has to consult the Data Owners and the DPO, collaborating in defining product/service specifications and the collection of relevant information. In this regard, it will be his/her responsibility to cooperate with the Data Controller in order to fulfil the obligation to conduct an appropriate Data protection Impact Assessment in all situations where it is required, as well as in carrying out the procedures for prior consultation with the Data Protection Authority when necessary.
Data Subject request management	The IDS must support the DPO in handling requests from data subjects. If a data subject sends a request to the area of his or her responsibility, in relation to his or her rights under the applicable legislation, the IDS is required to immediately notify the DPO and to work with the latter to promptly comply with the request, in accordance with the relevant policy adopted by the Company and any other operational instructions received in this regard. With reference to any requests concerning the specific area of expertise, he/she will be required to ensure that the operations of data are prompt and complete.

Organizational structures and relationships with third parties	The IDS must organize periodical meetings with third parties that may have been appointed by the Data Controller as Data Processors in relation to services and/or activities falling in the area/department assigned to the IDS, in order to verify the correct and timely implementation of the instructions provided to them.
Data Breach	The IDS must immediately notify the DPO in the event that he/she becomes aware, or has reason to suspect, that a data breach occurred or may occur, accidentally or maliciously, due to the destruction, loss unauthorized modification, disclosure or access to personal data subject to the control of the Company (Data Breach), in each case provided in the "Data Breach Management Policy" implemented by the competent Data Controller.

5.4 Data owner

Within the Privacy Organizational Model, the Data Owners represent the head of an area/department that processes personal data. Despite the opportunity to delegate, the Data Owner remains fully accountable for the tasks and responsibilities assigned within the policy. In the table below, some of the main tasks assigned to him/her:

Task	Description
1. Record of processing activities	• The Data Owner must update the Record of processing activities, by filling in every new data processing or modification to already mapped one, with reference to: o Categories of Data subjects: natural person to whom the data refer (e.g., employees, customers, prospects, etc.).

	○ Purpose of processing: reason for which the company collects personal data from individuals (e.g., sending advertising communication). ○ Categories of processed data: general, particular and/or judicial personal data. ○ Legal basis: indication of the legal ground to process personal data (e.g., performance of a contract of which the Data Subject is a party, consent of the data subject). ○ Recipients to whom the data are disclosed: indication, even as category, of the Data controllers (e.g., social security agencies), Data processors and Sub Processors to whom the data will be disclosed. ○ Retention periods: time frame during which the company processes data. ○ Security measures: the technical and organizational measures adopted to ensure data protection (e.g., encryption, access control). ○ Ownership: indication of the internal referent responsible for managing the data processing and keep it up to date. ○ Extra EU data transfers: information about the third Country(ies) to which the data are transferred, the specific recipients of the transfer and the relevant implemented guarantee (e.g., adequacy decisions, SCC.).
2. Privacy screening	• When (i) a new project or process that implies a personal data processing is defined or (ii) an existing processing activity is modified (e.g., there is a higher volume of personal data processed), the Data Owner must: ○ Carry out a Privacy Screening by collecting the needed information, even involving any competent

	referent of department (e.g., the DPO, the Information & IT security, Marketing/communication, HR, but also external subject involved in the process). o with the help of the competent Areas/Departments, collect the required information to complete the Privacy Screening. o after checking the information required are correct and complete, proceed with the completion of the Privacy Screening • At the end of the Privacy Screening, the Data Owner must identify potential risks related to the processing activities, in order to assist the competent function of the Data Controller, supported by the DPO, in the Data Protection Impact Assessment execution.
3. Data transfer impact assessment	• When a process activity implies a data transfer, the Data Owner must identify the Third Party and the Country to which the data must be transferred. • In case the Third Party is responsible to carry out the DTIA, the Data Owner acquires from the Third Party the DTIA and forwards it to the DPO to get an assessment of the adequacy of the DTIA. • With the support of the Head of Information & IT Security (if necessary), he/she fills in the DTIA, indicating, among others, the following information: o categories of Personal Data involved in the data transfer (e.g., personal identifiable information, personal health information, personal financial information, judicial data). o purpose(s) of processing and data transfer. o industry in which the processing occurs. o Country where data will be transferred.

	○ IT systems involved in the Data Transfer (e.g., systems that store Personal Data, systems with access to databases). ○ the technical measures in place / to be adopted for the data transfer with the support of the Head of Information & IT Security. ○ storage location of the transferred data. ○ actors involved in the Data Transfer (e.g., business functions, hosting provider, storage provider) and their respective roles in the processing activity (e.g., Controller, Processor, Sub-Processor). • Then the Data Owner: ○ shares the compiled DTIA with the DPO. ○ In case of negative outcome (high risk transfer) of the assessment, in collaboration with the data importer (the company transferring data) and with the support of the Head of Information & IT Security, identifies which supplementary measures (technical, organizational) could guarantee an adequate level of protection for personal data. ○ collaborates in implementing the necessary organizational measures defined. ○ communicates to the DPO any modification that could impact Personal Data processing and the DTIA outcome.
4. Privacy Notice	• The Data Owner must provide privacy notices to the data subjects, at the moment of when their data are collected or upon first contact with them, in order to let them know: ○ the identity and the contact details of the controller and, where applicable, of the controller's representative. ○ the contact details of the DPO, where applicable.

	○ the purposes of the processing for which the personal data are intended as well as the legal basis for the processing. ○ where the processing is based, the legitimate interests pursued by the controller or by a third party. ○ the recipients, or the categories of recipients, of the personal data. ○ where applicable, the fact that the controller intends to transfer personal data to a third country or international organization and the appropriate security measures.

5.5 Person in charge of processing

The person in charge of processing is the natural person (employees, collaborators and other figures) who materially carries out the processing operations on personal data. To fulfil their functions, it is necessary that the Human Resources and Organization Department appoint them and instruct them on the processing that they have to carry out, even in relation with the obligations related to the adoption of security measures. It is also necessary that they are provided with the relevant training by the DPO, in order to make them conscious of the risk related to the data processing. Finally, their activity is monitored by the respective Data Owner, as head of his/her own area/department, and, indirectly, at Country level, by the Internal Data Supervisor

5.6 Privacy Focal Points

The Privacy Focal Point is a role that may be defined in any Company as local point of contact for the Group DPO. If defined, he/she helps the Group DPO to monitor the local privacy compliance, by

- continuously verifying compliance status in his/her context of activity.
- reporting the Group DPO every privacy issue occurred.
- assisting the DPO in specific implementation on-site.

This role may be assigned to an Officer operating within the following Departments, depending on the organization of the Company concerned:

- Compliance.
- Legal.
- Information Technology.
- Security.

6. CONSEQUENCES OF POLICY VIOLATION

As a Prysmian employee, you are agreeing to uphold our commitment to ethical conduct and integrity and to abide by our Code of Ethics. 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.

7. REPORTING A POLICY VIOLATION

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

a) **the Integrity First Helpline;** 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 Code of Ethics or any other 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.
Lorem Ipsum

8. 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 Group Compliance 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.

9. RELATED DOCUMENTS

The following Procedures are related to this Policy and provide details on how the company intends to comply with GDPR requirements. They 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.**

a) Data Protection by Design and DPIA procedure;
b) Data subject rights procedure;
c) Vendor Management procedure;
d) Data Breach Incident Management procedure;
e) Procedure on the use of corporate IT tools and employer's supervisory powers;
f) System Administrator management procedure.

APPENDIX A – DEFINITIONS

Terms	Meaning
Personal data	Any information relating to an identified or identifiable natural person ("data subject"), even indirectly, by reference to any other information, including a name, an identification number, location data, an online identifier or a or more characteristic elements of its physical, physiological, genetic, psychic, economic, cultural or social identity.
Processing	Any operation, or set of operations, which is carried out on personal data or series of personal data, including by automated means, such as the collection, registration, organization, structuring, conservation, adaptation or modification, extraction, consultation, use, communication by transmission, diffusion or any other form of making available, comparison or interconnection, limitation, cancellation or destruction.
Data subject	The natural person identified or identifiable, directly, or indirectly, by personal data and in any case to whom the processed data refers.as
Data processor (or "Processor")	The natural or legal person (e.g., outsourcers, providers of services, consultants, distributors, and agents), public authority, agency or other body which processes personal data on behalf of the Controller.
Data Controller (or "Controller")	It means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data, also with respect to security aspects.
Persons in charge of processing	The natural persons, such as employees or personnel whom the data controller or processor has authorized in writing to carry out personal data processing operations.
The Data Protection Officer (or "DPO")	The person designated by the data controller or data processor to perform support and control, consultative, training and information functions in relation to the application of the Regulation itself. It cooperates with the Authority and constitutes the point of contact, also with respect to the Data Subjects, for matters connected to the processing of personal data.
Internal Data Supervisor	The person responsible for assisting the local management in setting the appropriate "tone at the top" of their business organization in order to

	comply with the Group's and local privacy requirements; he/she implements and manages the Global Privacy Program at a local level by maintaining day-to-day compliance procedures and controls.
Data Owner	The head of an area/department that processes personal data, who can delegate the fulfilling of privacy tasks to one or more member of his/her team. Despite the opportunity to delegate, the Data Owner remain fully accountable for the tasks and responsibilities assigned by the policy at stake.
Privacy Focal Point	The Privacy Focal Point is a role that may be defined in a Prysmian as local point of contact for the Group DPO. If defined, he/she helps the Group DPO to monitor the local privacy compliance
Third party	The natural or legal person other than the interested party, the owner, the manager and the persons in charge of processing
Consent	Any statement or action by which an interested party freely, specifically and in an informed and unambiguous manner indicates his consent to the processing of personal data concerning him
Personal data breach	Any breach of security resulting in the accidental or unlawful destruction, loss, unauthorized alteration or disclosure of, or access to, personal data transmitted, stored or otherwise processed

APPENDIX B – GENERAL PRINCIPLES

In order to protect the rights granted to data subjects, all personal data must be treated in accordance with the following principles:

- correctness and transparency: the data are processed in a correct and transparent manner for the data subject; in particular, the interested party must receive sufficient notice before carrying out any data processing and be constantly updated on any changes to what was initially specified.
- legitimacy: the data are collected and processed, with the exception of mandatory situations explicitly provided for by the Regulation, only if one or more of the legitimacy conditions defined in the Regulation are met.
- purpose limitation: data is collected only for specific, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.
- data minimization: the data is adequate, pertinent and limited to what is strictly necessary in relation to the purposes for which it is collected.
- accuracy: the data is accurate and, where necessary, updated. For this reason, it is necessary to take all the necessary measures to ensure that inaccurate data, in relation to the purposes for which they are processed, are cancelled, or rectified without delay.
- conservation limitation: the data are kept in a form that allows the identification of the interested parties for a period not exceeding that necessary to achieve the purposes for which they were collected and processed.
- integrity and confidentiality: the data is processed in such a way as to guarantee, by applying appropriate technical and organizational measures, an adequate level of security, in particular in terms of protection against unauthorized data processing, access, destruction, loss, modification or disclosure.
- accountability: the data controller must be able to demonstrate that adequate measures and processes have been adopted to guarantee compliance with the principles set out in the previous points and with the provisions of the GDPR.