Modello Organizzativo Privacy

APPROVATO DAL CONSIGLIO DI AMMINISTRAZIONE

DI PRYSMIAN S.p.A.

DEL 7 MAGGIO 2025

The planet's pathways

TABELLA DEI CONTENUTI

1. SCOPO E OBIETTIVO

La presente policy ha lo scopo di descrivere i principali ruoli in materia di privacy e protezione dei dati all'interno di Prysmian Group (di seguito, "Prysmian" o il "Gruppo") e di definire i relativi compiti e responsabilità in conformità alla normativa vigente in materia di protezione dei dati personali, con specifico riferimento al Regolamento (UE) 2016/679 (Regolamento generale sulla protezione dei dati, di seguito "GDPR" o "Regolamento"), nonchè fornire linee guida in merito alle azioni da intraprendere e alle procedure da attuare per garantire il coordinamento tra il Data Protection Officer (o "DPO") nominato da Prysmian e il punto di contatto locale designato presso ciascuna delle Società (di seguito, la "Società").

2. OWNERSHIP DELLA POLICY

Il DPO è il responsabile della presente Policy e ha il compito di occuparsi della sua revisione e aggiornamento periodici, al fine di garantire l'aderenza agli aggiornamenti organizzativi nonchè alle modifiche normative e regolamentari applicabili.

3. AMBITO DI APPLICAZIONE

La presente Policy si applica a tutti i dipendenti, stagisti, consulenti esterni, dirigenti e amministratori di tutte le entità giuridiche di Prysmian che rientrano nell'ambito di applicazione del GDPR (Articolo 3 GDPR). Eventuali esenzioni dall'applicazione di specifiche disposizioni della presente Policy devono essere valutate dal Gruppo Prysmian.
Le esenzioni saranno considerate eslusivamente se:

- Eventuali circostanze particolari non consentono l'attuazione di un requisito (ad esempio, il rischio di compromettere indagini in corso da parte di altre Autorità).
- Una legge o un regolamento locale che preveda un'eccezione.
- Controlli compensativi per mitigare il rischio.

4. LA TUA RESPONSABILITÀ IN QUALITÀ DI DIPENDENTE

La presente Policy richiede che tu:

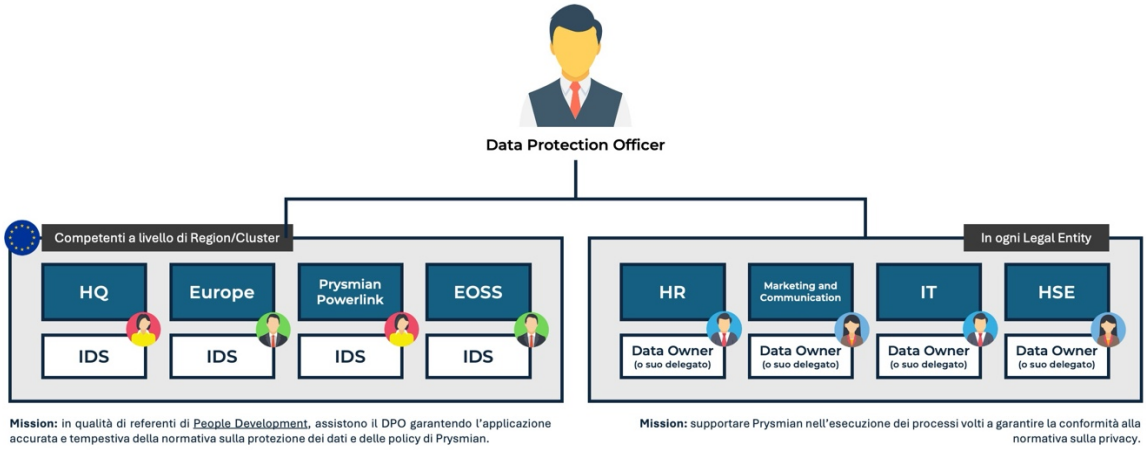
a) Legga, comprenda e rispetti i requisiti contenuti in questa Policy;
b) Rispetti il Codice Etico di Prysmian e ogni altra policy o procedura applicabile;

c) Segnali immediatamente, attraverso i canali appropriati indicati nella Sezione 6 della **Helpline Policy,** qualsiasi presunta violazione della presente Policy, sia se commessa da un dipendente di Prysmian che da uno soggetto esterno;
d) Ponga domande o segnali eventuali dubbi relativi alla presente Policy;
e) Completi, ove richiesto, i corsi di formazione assegnati relativi alla presente Policy.

5. REQUISITI DELLA POLICY - RUOLI

I principali ruoli in materia di privacy e protezione dei dati personali identificati e assegnati sono i seguenti:

- DPO: la persona designata dal Titolare o dal Responsabile del trattamento per monitorare la conformità al GDPR, alle altre disposizioni dell'Unione o degli Stati membri in materia di protezione dei dati, nonchè alle policy adottate dal Titolare o dal Responsabile del trattamento in materia di protezione dei dati personali, compresa l'attribuzione delle responsabilità, le attività di sensibilizzazione e formazione del personale coinvolto nelle operazioni di trattamento, nonchè i relativi audit agli Interessati per le questioni connesse al trattamento dei dati personali. All'interno di Prysmian, il ruolo del DPO varia a seconda che sia svolto dal DPO formalmente nominato in un determinato Paese o dal DPO che opera a livello di Gruppo secondo quanto previsto dal Modello Organizzativo Privacy. Di seguito sono elencati i compiti del DPO, come definiti dal GDPR, validi per i Paesi in cui è nominato a livello locale, e successivamente viene fornita una descrizione dei compiti svolti dal DPO di Gruppo.
- Internal Data Supervisor: la persona incaricata di assistere il management locale nell'adozione, implementazione e gestione, a livello di Regione/Cluster, di standard, policy, procedure e processi, in linea con quanto stabilito dal DPO di Gruppo.
- Data Owner: il responsabile di un'area o dipartimento che tratta dati personali, che può delegare l'esecuzione di specifici compiti in ambito privacy a uno o più membri del proprio team. Nonostante la possibilità di delegare, il Data Owner rimane pienamente responsabile dei compiti e delle responsabilità che gli sono stati assegnati dalla policy di riferimento.



Le indicazioni contenute in questo documento sono state redatte sulla base di:

- decisioni adottate dalle Autorità locali competenti per la protezione dei dati personali (di seguito, l'"Autorità" o "DPA");
- best practice di settore sviluppate nel corso degli anni;
- Linee guida sui Responsabili della Protezione dei Dati (WP243), adottate dal Gruppo di Lavoro Articolo 29 (di seguito, "WP29") il 5 aprile 2017 (di seguito, le "Linee guida").

5.1 Il ruolo di DPO secondo il GDPR

Il presente paragrafo illustra le principali caratteristiche del ruolo del DPO così come previsto dal GDPR. Esso si applica solo alle Legal Entity del Gruppo in cui il DPO è formalmente nominato. In tale contesto, il DPO è responsabile delle seguenti attività:

- fornire consulenza alla Società in merito agli obblighi previsti dalla normativa in materia di protezione dei dati personali;
- monitorare (e garantire) il rispetto della normativa vigente;
- fungere da punto di contatto per le Autorità di controllo competenti, ossia le autorità locali/principali competenti della protezione dei dati personali.

Il DPO deve essere nominato tenendo conto delle sue qualità professionali, in particolare in base alla profonda conoscenza della normativa e delle prassi in materia di protezione dei dati personali, nonchè della capacità di svolgere in modo efficace i compiti affidatigli.

Le conoscenze specialistiche devono essere valutate sulla base delle tipologie di trattamento effettuate a livello aziendale, in particolare considerando la sensibilità, la complessità e la quantità dei dati oggetto di trattamento.

Le competenze richieste includono:

- conoscenza approfondita della normative nazionali ed europee in materia di protezione e sicurezza dei dati personali.
- consapevolezza delle operazioni di trattamento svolte dalle diverse funzioni aziendali.
- competenze in ambito informatico e in materia di misure di sicurezza.
- conoscenza specifica del settore di mercato in cui opera la Società e della sua organizzazione interna.
- capacità di promuovere la cultura della protezione dei dati a livello aziendale, contribuendo all'attuazione degli elementi chiave del Regolamento, quali i principi fondamentali del trattamento, i diritti degli interessati, i criteri di privacy-by-design e privacy-by-default, la redazione di registri delle attività di trattamento adeguati, l'adozione di misure di sicurezza appropriate per la gestione dei rischi individuati e la corretta gestione di eventuali violazioni di dati personali.

5.1.1 Responsabilità del DPO

I seguenti compiti devono essere svolti dai DPO nominato ai sensi del GDPR, fermo restando che l'estensione delle responsabilità assegnate è lasciata alla discrezionalità del titolare del trattamento (o del responsabile), tenendo conto della sensibilità, complessità e quantità dei dati personali coinvolti. In ogni caso, mediante nomina o delibera equivalente degli organi societari competenti, deve essere garantito che il DPO svolga almeno le seguenti responsabilità:

Area	Responsabilità	Frequenza	Evidenze	Riferimenti
1. Policy, procedure e modelli	• Pubblicazione e aggiornamento di policy, procedure e ogni altra documentazione o modello necessario (ad esempio, lettere di nomina degli Amministratori di sistema, istruzioni agli incaricati del trattamento). • Comunicazione adeguata di tale documentazione all'interno della Società (ad esempio, pubblicazione sulla intranet).	All'occorrenza	Set di policy approvate	Set di policy approvate

2. Data Owner	• Definire il documento per assegnare le responsabilità al Data Owner.	Al cambiamento delle responsabilità del Data Owner	Email/Documento al Data Owner	Modello organizzativo privacy
3. Istruzioni agli incaricati del trattamento	• Definire e aggiornare il modello di istruzioni per gli incaricati del trattamento. • Comunicare tali istruzioni in modo appropriato all'interno della Società (ad esempio, pubblicandole sull'intranet).	Annuale (se necessario)	Modello di istruzioni per incaricati del trattamento	Modello organizzativo privacy

4. Amministratori di sistema	• Definire e aggiornare il modello di nomina per gli amministratori di sistema e condividerlo con la Funzione Information & IT Security. • Verificare che l'identificazione e la nomina degli amministratori di sistema sia effettuate dalla Funzione Information & IT Security. • Ove necessario, supportare la Funzione 'Information & IT Security nell'adattamento del modello di nomina, tenendo conto dei sistemi gestiti dall'Amministratore di Sistema e dei dati personali trattati.	• Se necessario (l'aggiornamento del modello di nomina) • Annuale (verifica delle nomine)	Modello di nomina dell'amministratore di sistema	Modello organizzativo privacy
5. Formazione e sensibilizzazione	• Fornire una formazione specifica a tutte le funzioni aziendali, predisporre e aggiornare il materiale formativo sulla privacy e sulla protezione dei dati. • Pianificare ed erogare le sessioni di formazione.	All'occorrenza	Materiale formativo sul GDPR	Modello organizzativo privacy

6. Registro delle attività di trattamento	• Garantire l'aggiornamento periodico dei registri del trattamento (sia in qualità di Titolare che di Responsabile del trattamento, ove applicabile).	• Se necessario (ad esempio, in tutti i casi in cui un trattamento in atto viene modificato in modo sostanziale o viene intrapresa una nuova attività di trattamento); • Almeno annuale	• Registro del trattamento in qualità di Titolare del trattamento • Registro del trattamento in qualità di Responsabile del trattamento	Registro delle attività di trattamento
7. Informative e consensi privacy	• Mappare tutti i canali di raccolta dei dati personali, ad esempio siti web, schede prodotto o moduli informativi. • Per ogni canale identificato, preparare le relative informative privacy e i moduli di consenso, se necessario. • Aggiornare tutte le informative privacy e i moduli di consenso. • Verificare la corretta acquisizione e gestione dei consensi richiesti.	• Nel caso in cui venga implementato un nuovo canale/metodo di raccolta dati; • Annuale (se necessario)	• Mappatura dei canali di raccolta dei dati personali; • Informative privacy; • Moduli di consenso.	Modello organizzativo privacy
8. Diritti degli interessati	• Analizzare e rispondere alle richieste degli interessati in collaborazione con il Data Owner. • Mantenere un elenco aggiornato delle richieste ricevute.	Ogni volta che si riceve una richiesta dell'interessato	• Elenco delle richieste di esercizio dei diritti	Procedura sui diritti degli interessati

			• Corrispondenza con gli interessati	
9. Trasferimenti di dati personali extra-UE	• Mappare i trasferimenti di dati personali extra-UE. • Verificare che i trasferimenti di dati personali al di fuori dello Spazio Economico Europeo siano effettuati in conformità alle disposizioni applicabili. • Eseguire periodicamente dei Data Transfer Impact Assessment.	• In tutti i casi in cui viene intrapreso un nuovo trattamento di dati che implica un trasferimento di dati extra-UE; • Annuale (se necessario)	• Mappatura dei trasferimenti di dati personali al di fuori dell'UE • Data Transfer Impact Assessment	Trasferimenti di dati personali
10. Privacy by design e by default	• Mantenere un elenco aggiornato degli screening privacy effettuati dai Data Owner. • Verificare il completamento tempestivo degli screening privacy effettuati dai Data Owner. • Valutare gli screening privacy ricevuti.	Ogni volta che viene pianificato un nuovo progetto o processo che comporta il trattamento dei dati personali	• Scheda di screening privacy • Elenco aggiornato degli screening	Procedura sulla Data Protection by Design e DPIA
11. Valutazione d'impatto sulla protezione dei dati	• Supportare le funzioni competenti di Prysmian nell'esecuzione delle valutazioni di impatto sulla protezione dei dati sul trattamento dei dati personali.	Ogni volta che un Privacy screening richiede l'esecuzione di una DPIA	• DPIA • Elenco aggiornato delle DPIA eseguite	Procedura sulla Data Protection by Design e DPIA.

	• Monitorare l'esecuzione del piano d'azione, se definito nella DPIA. • Mantenere un elenco aggiornato delle DPIA eseguite.			
12. Data breach	• Valutazioni di data breach. • Mantenere un elenco aggiornato degli eventi di violazione dei dati potenziali ed effettivi e delle relative valutazioni.	Ogni volta che si verifica un evento	• Valutazione delle potenziali ed effettive violazioni dei dati • Elenco aggiornato delle violazioni di dati potenziali ed effettive	Procedura sulla gestione degli incidenti e delle violazioni di dati personali (data breach incident management)
13. Conservazione dei dati	• Valutare l'adeguatezza dei periodi di conservazione identificati dal Data Owner. • Verificare che sia in atto un processo strutturato per garantire la cancellazione (o l'anonimizzazione) dei dati personali una volta terminato il periodo di conservazione identificato.	• In tutte le aree in cui viene intrapreso un nuovo trattamento di dati, per il quale deve essere identificato un periodo di conservazione dei dati appropriato; • Annuale	Identificazione del periodo di conservazione dei dati	Procedura sulla conservazione dei dati personali

14. Misure di sicurezza	• Verificare l'attuazione di adeguate misure di sicurezza tecniche e organizzative per proteggere adeguatamente i dati personali.	Annuale	Misure minime di sicurezza	Modello organizzativo privacy
15. Responsabili del trattamento dei dati	• Aiutare i Data Owner a verificare che i fornitori di servizi esterni/outsourcer da nominare come responsabili del trattamento offrano adeguate garanzie per mettere in atto misure tecniche e organizzative idonee affinché il trattamento sia conforme al GDPR e protegga i diritti delle persone. • Mettere a disposizione del Data Owneril modello per la designazione a responsabile del trattamento. • Quando necessario, supporta i titolari del contratto nel processo di nomina dei fornitori come responsabili del trattamento dei dati quando questi trattano dati personali per conto della Società. In particolare, il DPO fornisce supporto per adattare il contratto di nomina a responsabile del	Attività continua	• Modello di nomina a Responsabile del trattamento • Repository degli accordi di nomina a responsabile del trattamento firmati • Elenco aggiornato dei responsabili del trattamento • Piano di audit • Lista di controllo per l'audit dei responsabili del trattamento • Report di audit	Modello organizzativo privacy e procedura sulla gestione dei fornitori (Vendor Management)

	trattamento allo specifico servizio fornito e alle caratteristiche del trattamento dei dati. • Mantenere un elenco aggiornato dei responsabili del trattamento nominati. • Mantenere un file aggiornato contenente copie del contratto di nomina a responsabile del trattamento. • Definizione ed esecuzione di un piano di audit annuale sui Responsabili del trattamento più rilevanti.			
16. Controlli di secondo livello	Eseguire controlli di secondo livello sui Data Owner per verificare le seguenti aree: • Registri delle attività di trattamento; • Informative privacy e consensi; • Trasferimenti di dati extra-UE; • Privacy by design e by default; • Conservazione dei dati; • Misure di sicurezza;	Annuale	Elenco dei controlli di secondo livello • Report	Modello organizzativo privacy

	• Responsabili del trattamento dei dati.			
17. Rapporto con l'Autorità	• Comunicazione all'Autorità di controllo sulla protezione dei dati personali ed eventuale condivisione dei documenti in caso di verifica da parte dell'Autorità, o di consultazione preventiva ai sensi dell'art. 36 GDPR.	Ogni volta che la comunicazione viene inviata/ricevuta.	Copia della comunicazione	Modello organizzativo privacy
18. Reportistica	• Preparazione della relazione annuale al Consiglio di amministrazione o al Comitato rischi e controllo.	Annuale	Relazione del DPO	• Modello organizzativo privacy • Monitoraggio e reportistica

Nel corso della sua attività di vigilanza, il DPO deve condurre un'attenta analisi dei rischi connessi al trattamento, tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento. In particolare, il DPO è tenuto a stabilire un

ordine di priorità nell'esercizio delle sue funzioni di vigilanza, concentrandosi maggiormente sulle questioni che, in base alla sua prudente valutazione, potrebbero comportare maggiori rischi in termini di protezione dei dati.

5.1.2 DPO interno ed esterno

La persona designata a svolgere il ruolo di DPO, anche attraverso la creazione di un ufficio e di un team dedicato, può essere nominata all'interno o all'esterno dell'organizzazione del titolare e del responsabile del trattamento.

- DPO interno: se il DPO è scelto tra persone con cui la Società intrattiene rapporti di lavoro, è essenziale che la persona selezionata non ricopra posizioni, soprattutto manageriali, che possano dare origine a conflitti di interesse. Pertanto, il DPO interno non può svolgere contemporaneamente il ruolo di DPO e di responsabile di una funzione aziendale che stabilisce le finalità e i mezzi del trattamento dei dati.
- DPO esterno: Il ruolo di DPO può essere svolto anche sulla base di un contratto di servizio stipulato con una persona fisica o giuridica esterna alla società del titolare del trattamento. Anche in questo caso, nella scelta del soggetto da nominare, devono essere rispettati tutti i requisiti soggettivi e oggettivi previsti dalla normativa vigente, come meglio specificato nella presente Policy e nelle Linee Guida del WP29 (ora EDPB).

5.1.3 Contatto DPO

I dati di contatto del DPO, come l'indirizzo postale e un indirizzo e-mail specifico, devono essere:

- incluse in tutte le Informative fornite agli interessati, ai sensi degli artt. 13 e 14 GDPR;
- pubblicato in modo tale che l'Autorità, o altre autorità di vigilanza, possano facilmente contattare il DPO;
- comunicate all'Autorità e, secondo le buone prassi, anche a tutti i dipendenti (ad esempio, tramite l'intranet aziendale) e ad eventuali terzi coinvolti.

5.1.4 Garanzie per l'ufficio del DPO

Per consentire al DPO di adempiere ai propri compiti in modo autonomo, indipendente e conforme alla normativa vigente, il Titolare del trattamento deve mettere a disposizione del DPO tutte le risorse (ad esempio finanziarie, di personale, di conoscenze e di formazione

continua) necessarie per un'esecuzione adeguata, efficiente e tempestiva di tali compiti. Questo requisito è soddisfatto se il DPO può disporre di:

- assistenza attiva da parte del senior management (ad esempio, il Consiglio di amministrazione).
- tempo sufficiente per svolgere i compiti di cui è responsabile (in particolare, per evitare che le attività affidate al DPO finiscano per essere trascurate a causa di conflitti con altre priorità aziendali).
- un adeguato supporto in termini di risorse finanziarie, infrastrutture (uffici, attrezzature, strumenti) e, se opportuno, personale interno e consulenti esterni.
- comunicazione ufficiale a tutto il personale di Prysmian della nomina del DPO, per assicurare che la presenza e le funzioni del DPO siano ben note all'interno della Società.
- accesso garantito ad altri servizi (risorse umane, ufficio legale, IT, sicurezza, ecc.) per poter ricevere tutta l'assistenza e le informazioni essenziali.
- formazione continua, per rimanere costantemente aggiornato sugli sviluppi nel settore della protezione dei dati e aumentare gradualmente il proprio livello di competenze.
- creazione di un ufficio o di un gruppo di lavoro del DPO (composto dal DPO e da personale di supporto adeguato), ove necessario o opportuno in considerazione delle dimensioni e della struttura della Società. In questi casi, è consigliabile definire con precisione la struttura interna del gruppo di lavoro, nonché i singoli compiti e le responsabilità.
- senza alcuna istruzione da parte del titolare (o responsabile) del trattamento che lo ha nominato, senza alcuna interferenza da parte di altre funzioni aziendali, compresa l'alta direzione.
- sapendo di non poter essere sanzionato in alcun modo (o intimidito) o rimosso dall'incarico in relazione all'esercizio delle sue funzioni.
- con la garanzia di riferire direttamente agli organi di governo (es. CEO o Consiglio di Amministrazione). È possibile che il ruolo di DPO sia affidato a una persona che già svolge mansioni diverse da quelle tipiche di questa posizione (ad esempio, Chief Compliance Officer); in questo caso, è fondamentale organizzare la struttura di governance aziendale in modo tale che questa persona, in qualità di DPO, possa

riferire direttamente ai vertici del titolare (o del responsabile) del trattamento, anche se questa condizione non è prevista per l'altra carica che la persona ricopre.

5.1.5 Impegno del DPO

È essenziale che il Responsabile della protezione dei dati e il suo eventuale team siano coinvolti il prima possibile in qualsiasi questione relativa al trattamento dei dati personali.
Inoltre, in considerazione della necessità di un dialogo diretto con i vertici aziendali, è necessario che il DPO sia puntualmente invitato a partecipare ai gruppi di lavoro che di volta in volta si occupano delle attività di trattamento. A tal fine, occorre garantire che:

- che il DPO possa partecipare regolarmente alle riunioni di gestione in cui si discutono questioni che potrebbero avere un impatto sulla sicurezza dei dati e sui diritti degli interessati.
- che il DPO disponga di tutte le informazioni necessarie per poter fornire una consulenza adeguata e tempestiva ogni qualvolta si debbano prendere decisioni relative al trattamento dei dati.
- che il parere del DPO sia sempre tenuto in debita considerazione e che le ragioni a sostegno della decisione presa dalla Società siano documentate quando la decisione è sostenuta dal DPO.
- che il DPO sia immediatamente consultato ogni volta che si verifica una violazione dei dati o qualsiasi altro evento rilevante, o quando si sospetta il verificarsi di una violazione dei dati o di un evento

5.2 DPO di Gruppo

Per le altre società del Gruppo in cui il DPO non è formalmente nominato, il DPO di Prysmian assicura e monitora la conformità alla normativa privacy verificando che le policy, le procedure e i documenti di ciascuna società siano conformi a tutti gli standard del Gruppo e che siano coerenti con il documento corrispondente in ciascuna legal entity del Gruppo.
Nel corso delle suddette attività, il DPO di Gruppo è responsabile del monitoraggio e del coordinamento delle attività dei seguenti ruoli privacy per garantire la conformità alla normativa applicabile a livello di Gruppo:

- Internal Data Supervisor a livello europeo.

- Privacy Focal Point, che può corrispondere a un funzionario che opera all'interno di uno dei seguenti dipartimenti, a seconda dell'organizzazione dell'azienda interessata:
  - Compliance,
  - Legal,
  - Information Technology,
  - Security.

5.3 Internal data supervisor

Gli "Internal data supervisor" ("IDS") rappresentano un ruolo nominato dall'esecutivo o dal comitato locale competente, in accordo con il GDPR. I criteri di valutazione per la designazione dipendono anche dall'attività interna del Paese, dai dipartimenti, dalla regione, dalla struttura delle società controllate e dalla complessità dell'organizzazione.
L'IDS è responsabile di supportare il management locale nell'istituzione del corretto "*tone at the top*" della propria organizzazione aziendale, al fine di garantire il rispetto dei requisiti privacy del Gruppo e di quelli locali.
IDS implementa e gestisce il Global Privacy Program a livello locale, mantenendo operative le procedure e i controlli di compliance quotidiani.
L'IDS ha la responsabilità di controllare, ai sensi di legge, che i trattamenti di dati connessi alle attività svolte dalla sua funzione, e le altre attività che il Titolare del trattamento deciderà di affidargli in futuro, avvengano nel pieno rispetto della normativa applicabile, comprese le disposizioni in materia emanate dalle competenti Autorità di protezione dei dati.
L'elenco completo delle attività di trattamento dei dati personali delegate alla sua area di responsabilità è riportato nel Registro delle attività di trattamento predisposto e aggiornato periodicamente dal Titolare.
In particolare

Compito	Descrizione
1. Gestione del registro delle attività di trattamento	• L'IDS deve: o aiutare il dipartimento aziendale competente nella regolare tenuta del Registro delle attività di trattamento. A tal fine, trasmetterà a tale dipartimento

	tutte le informazioni relative al trattamento dei dati personali effettuato all'interno del Dipartimento di cui è responsabile, nonché qualsiasi modifica relativa al trattamento e ai mezzi con cui viene effettuato, ed eventuali terzi coinvolti. o Assicurarsi che tali dati siano essenziali e pertinenti per realizzare gli scopi specifici della sua area di responsabilità. Se questi principi (essenzialità e pertinenza dei dati) non sono soddisfatti, deve interrompere il trattamento dopo aver consultato il Responsabile della protezione dei dati.
2. Categorie particolari di dati personali	Qualora sia necessario il trattamento di tali dati personali, l'IDS deve contattare il DPO ed eventualmente il dipartimento IT per determinare le modalità di trattamento più appropriate.

Obblighi legali	• L'IDS deve garantire che tutte le attività di trattamento dei dati che rientrano nella sua area di responsabilità siano svolte nel rispetto degli obblighi di legge. In particolare, per quanto riguarda gli interessati, deve garantire l'adempimento degli obblighi relativi a: o fornitura di informazioni rilevanti, o richiesta di consenso, quando necessario, o esistenza di un'adeguata base giuridica per il trattamento, o esercizio dei diritti garantiti agli interessati, in particolare quando il trattamento riguarda dati sensibili o dati relativi a minori. • Nel caso in cui sorgano nuovi requisiti per il trattamento o emergano potenziali condizioni di inadeguata conformità alle disposizioni di legge, ha la responsabilità di consultare tempestivamente i Titolari e il DPO per determinare le opportune azioni correttive da intraprendere, compresa l'esecuzione di una Valutazione d'Impatto sulla Protezione dei Dati, in conformità con la relativa politica adottata dalla Società.
Misure di sicurezza tecniche e organizzative	L'IDS deve verificare che i dati personali trattati nell'ambito della sua area di responsabilità siano mantenuti sicuri e controllati in modo da ridurre al minimo il rischio di distruzione o perdita, compreso l'accesso accidentale o non autorizzato, o il trattamento non autorizzato o non conforme allo scopo della raccolta dei dati. Dovrà inoltre verificare che vengano attuate misure adeguate per la sicurezza del trattamento.

Incaricato del trattamento	• L'IDS deve:
	  o coordinare le attività del personale (dipendenti, stagisti, consulenti, ecc.) che effettua il trattamento dei dati personali nell'ambito della propria area di responsabilità e verificare che sia stato debitamente autorizzato a svolgere le relative operazioni di trattamento e che riceva le necessarie istruzioni sugli obblighi da adempiere nello svolgimento dei compiti assegnati.
	  o monitorare il puntuale rispetto delle istruzioni che il Titolare del trattamento ha fornito ai dipendenti che hanno accesso ai dati personali o che sono coinvolti nel loro trattamento.
	• Quando necessario, in accordo con il DPO, può stabilire istruzioni diversificate da fornire all'incaricato del trattamento in base agli ambiti operativi di sua competenza e alle attività specifiche assegnate.
	• Informerà tempestivamente il DPO qualora venga a conoscenza che uno o più incaricati del trattamento, anche se non operanti sotto la sua responsabilità, abbiano violato l'obbligo di segretezza, o abbiano commesso azioni o violazioni gravi che possano in qualche modo compromettere la sicurezza dei dati o delle banche dati.

Formazione e sensibilizzazione	L'IDS deve monitorare il rispetto delle procedure e delle istruzioni interne e deve contribuire a garantire la consapevolezza sui temi previsti dal piano di formazione. Ha la responsabilità di aumentare l'attenzione dei propri colleghi in relazione alla protezione dei dati personali e, più in generale, alla corretta gestione dei dati aziendali al fine di ridurre e minimizzare i rischi.

Applicazione dei principi di privacy-by-design e by-default	Al fine di garantire che il trattamento dei dati personali avvenga in conformità ai principi e ai requisiti legali stabiliti dalla legislazione applicabile in materia di protezione dei dati, IDS deve assicurare che tutti i Responsabili del trattamento dei dati che operano sotto la sua responsabilità operino secondo i principi della privacy by design e della privacy by default. Lo stesso obbligo deve essere assolto anche per quanto riguarda la protezione dei diritti degli interessati quando si innovano i processi aziendali e si definiscono e lanciano nuovi prodotti e servizi, includendo questa valutazione come fase strutturale del processo stesso. Nel valutare questi aspetti, deve consultare i Data Owner e il DPO, collaborando alla definizione delle specifiche del prodotto/servizio e alla raccolta delle informazioni rilevanti. A questo proposito, sarà sua responsabilità collaborare con il Titolare del trattamento per adempiere all'obbligo di condurre un'adeguata Valutazione d'impatto sulla protezione dei dati in tutte le situazioni in cui è richiesta, nonché per espletare le procedure di consultazione preventiva dell'Autorità Garante per la protezione dei dati personali quando necessario.
Gestione delle richieste degli interessati	L'IDS deve supportare il DPO nella gestione delle richieste degli interessati. Nel caso in cui un interessato invii una richiesta all'area di propria competenza, in relazione ai propri diritti ai sensi della normativa vigente, l'IDS è tenuto a darne immediata comunicazione al DPO e a collaborare con quest'ultimo per dare tempestivamente seguito alla richiesta, in conformità alla policy in materia adottata dalla Società e ad eventuali altre istruzioni operative ricevute in merito. Con riferimento ad eventuali richieste riguardanti la specifica area di competenza, egli sarà tenuto a garantire che le operazioni di trattamento dei dati siano tempestive e complete.

Strutture organizzative e rapporti con terzi	L'IDS deve organizzare incontri periodici con i soggetti terzi eventualmente nominati dal Titolare del trattamento quali Responsabili del trattamento in relazione a servizi e/o attività rientranti nell'area/reparto assegnato all'IDS, al fine di verificare la corretta e puntuale attuazione delle istruzioni loro impartite.
Data breach	L'IDS deve informare immediatamente il DPO nel caso in cui venga a conoscenza, o abbia motivo di sospettare, che si sia verificata o possa verificarsi un data breach, accidentale o doloso, a causa della distruzione, della perdita, della modifica non autorizzata, della divulgazione o dell'accesso ai dati personali soggetti al controllo della Società (Data Breach), in ogni caso previsto dalla "Data Breach Management Policy" implementata dal Titolare del trattamento competente.

5.4 Data owner

Nel Modello Organizzativo Privacy, i Data Owner sono i soggetti responsabili di un'area/reparto che tratta dati personali. Nonostante l'opportunità di delegare, il Data Owner rimane pienamente responsabile dei compiti e delle responsabilità assegnati nelle policy.
Nella tabella seguente sono riportati alcuni dei principali compiti a lui assegnati

Task	Descrizione
1. Registro dei trattamento	• Il Data Owner deve aggiornare il Registro delle attività del trattamento, inserendo ogni nuovo trattamento di dati o modifica di uno già mappato, con riferimento a: o Categorie dei soggetti interessati: persone fisiche a cui si riferiscono i dati (ad esempio, dipendenti, clienti, prospect, ecc.).

	○ Finalità del trattamento: ragioni per cui la Società raccoglie i dati personali degli interessati (ad esempio, l'invio di comunicazioni commerciali). ○ Categorie di dati trattati: dati personali generali, particolari e/o giudiziari. ○ Base giuridica: indicazione della condizione di liceità che giustifica il trattamento dei dati personali (ad esempio, l'esecuzione di un contratto di cui l'interessato è parte, il consenso dell'interessato). ○ Destinatari: indicazione, anche per categorie, dei titolari del trattamento (es. enti previdenziali), dei responsabili e dei sub-responsabili del trattamento a cui saranno comunicati i dati. ○ Periodi di conservazione: periodo di tempo durante il quale la Società tratta i dati. ○ Misure di sicurezza: le misure tecniche e organizzative adottate per garantire la protezione dei dati (ad esempio, crittografia, controllo degli accessi). ○ Ownership: indicazione del referente interno responsabile della gestione del trattamento dei dati e del loro aggiornamento. ○ Trasferimenti di dati extra UE: informazioni sul/i Paese/i terzo/i verso cui i dati sono trasferiti, sui destinatari specifici del trasferimento e sulla relativa garanzia attuata (ad esempio, decisioni di adeguatezza, SCC).
2. Privacy screening	• Quando (i) viene definito un nuovo progetto o processo che implica un trattamento di dati personali o (ii) viene modificata un'attività di trattamento esistente (ad esempio, viene trattata una quantità maggiore di dati personali), il Data Owner deve:

	○ Effettuare un Privacy Screening raccogliendo le informazioni necessarie, anche coinvolgendo qualsiasi referente competente del dipartimento (ad esempio, il DPO, la funzione Information & IT security, la funzione Marketing/Comunicazione, la funzione HR, ma anche soggetti esterni coinvolti nel processo). ○ con l'aiuto delle aree/dipartimenti competenti, raccogliere le informazioni necessarie per completare il Privacy Screening. ○ dopo aver verificato la correttezza e la completezza delle informazioni richieste, procedere con la compilazione del Privacy Screening • Al termine del Privacy Screening, il Data Owner deve identificare i potenziali rischi connessi alle attività di trattamento, al fine di assistere la funzione competente del Titolare del Trattamento, supportata dal DPO, nell'esecuzione della Valutazione di Impatto sulla Protezione dei Dati (DPIA).
3. Valutazione d'impatto del trasferimento dei dati (DTIA)	• Quando un'attività di processo implica un trasferimento di dati, il Data Owner deve identificare la Terza Parte e il Paese in cui i dati devono essere trasferiti. • Nel caso in cui la Terza Parte sia responsabile dell'esecuzione della DTIA, il Data Owner acquisisce dalla Terza Parte la DTIA e la trasmette al DPO per ottenere una valutazione dell'adeguatezza della DTIA. • Con il supporto del Responsabile della Sicurezza Informatica (se necessario), compila la DTIA, indicando, tra l'altro, le seguenti informazioni: ○ categorie di dati personali coinvolti nel trasferimento dei dati (ad esempio, informazioni personali

	identificabili, informazioni sanitarie personali, informazioni finanziarie personali, dati giudiziari). o finalità del trattamento e trasferimento dei dati. o *industry* nell'ambito della quale viene posto in essere il trattamento. o Paese in cui i dati saranno trasferiti. o sistemi IT coinvolti nel trasferimento dei dati (ad esempio, sistemi che memorizzano i dati personali, sistemi con accesso a banche dati). o le misure tecniche in atto/da adottare per il trasferimento dei dati con il supporto del Responsabile della Sicurezza Informatica. o località di memorizzazione dei dati trasferiti. o soggetti coinvolti nel trasferimento dei dati (ad esempio, funzioni aziendali, hosting provider, storage provider) e i rispettivi ruoli nell'attività di trattamento (ad esempio, titolare del trattamento, responsabile del trattamento, sub-responsabile). • Poi il Data Owner: o condivide la DTIA compilata con il DPO. o In caso di esito negativo (trasferimento ad alto rischio) della DTIA, in collaborazione con il soggetto che importa i dati (la società che trasferisce i dati) e con il supporto del Responsabile della Sicurezza Informatica, individua quali misure integrative (tecniche, organizzative) possano garantire un adeguato livello di protezione dei dati personali. o collabora all'attuazione delle necessarie misure organizzative definite. o comunica al DPO qualsiasi modifica che possa avere un impatto sul trattamento dei dati personali e sull'esito della DTIA.

4. Informativa privacy	• Il Data Owner deve fornire l'informativa privacy agli interessati, al momento della raccolta dei loro dati o al primo contatto con loro, per metterli al corrente: o l'identità e i dati di contatto del titolare del tratatmento e, se del caso, del suo rappresentante. o i dati di contatto del DPO, ove applicabile. o le finalità del trattamento dei dati personali e la base giuridica del trattamento. o qualora il trattamento si basi sui legittimi interessi perseguiti dal titolare del trattamento o da un terzo. o i destinatari, o le categorie di destinatari, dei dati personali. o se del caso, il fatto che il titolare del trattamento intende trasferire i dati personali a un paese terzo o a un'organizzazione internazionale e le misure di sicurezza appropriate.

5.5 Incaricato del trattamento

L'incaricato del trattamento è la persona fisica (dipendenti, collaboratori e altre figure) che esegue materialmente le operazioni di trattamento dei dati personali. Per l'espletamento delle loro funzioni è necessario che la funzione Risorse Umane e Organizzazione li nomini e li istruisca sui trattamenti che devono effettuare, anche in relazione agli obblighi connessi all'adozione di misure di sicurezza. È inoltre necessario che venga fornita loro la relativa formazione da parte del DPO, al fine di renderli consapevoli del rischio connesso al trattamento dei dati. Infine, la loro attività è monitorata dal rispettivo Data Owner, in qualità di responsabile della propria area/reparto, e, indirettamente, a livello di Paese, dall'Internal Data Supervisor.

5.6 Privacy Focal Point

Il Privacy Focal Point è un ruolo che può essere definito in ogni società come punto di contatto a livello locale per il DPO di Gruppo. Se definito, aiuta il DPO di Gruppo a monitorare la conformità privacy a livello locale, tramite le seguenti azioni:

- verificare continuamente lo stato di conformità nel proprio contesto di attività.
- segnalare al DPO del Gruppo ogni problema impattate l'aspetto privacy.
- assistere il DPO nell'attuazioni specifiche in loco.

Questo ruolo può essere assegnato a un funzionario che opera all'interno dei seguenti dipartimenti, a seconda dell'organizzazione della società interessata:

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

6. CONSEGUENZE DELLA VIOLAZIONE DELLA POLITICA

In qualità di dipendente di Prysmian, accetti di sostenere il nostro impegno alla condotta etica e all'integrità e di rispettare il nostro Codice Etico. I dipendenti di Prysmian che violano questo impegno o non rispettano la presente Policy saranno soggetti a procedure disciplinari, incluso il possibile licenziamento, e a qualsiasi altra azione legale necessaria per proteggere gli interessi e la reputazione di Prysmian, in linea con la legislazione vigente

7. SEGNALAZIONE DI UNA VIOLAZIONE DELLA POLITICA

In qualità di dipendenti di Prysmian, siete tenuti a segnalare qualsiasi violazione della Policy a:

a) **the Integrity First Helpline;** oppure
b) il vostro Team Compliance regionale o gli altri soggetti designati indicati nella sezione 6.1 della **Helpline Policy**.

È severamente vietata qualsiasi forma di ritorsione, comprese minacce e tentativi di ritorsione. Prysmian si impegna a garantire che tutti i dipendenti siano liberi di rivelare qualsiasi violazione, reale o presunta, del Codice Etico di Prysmian o di qualsiasi altra policy o procedura aziendale, nella misura in cui abbiano ragionevoli motivi per ritenere che le questioni segnalate siano reali. Non si subiranno ripercussioni negative o ritorsioni sul posto

di lavoro, né sul piano personale né su quello professionale, per aver sollevato una preoccupazione valida e legittima.

8. AUDIT, MONITORAGGIO E MIGLIORAMENTO CONTINUO

Il Responsabile della presente Policy ha la responsabilità di effettuare revisioni e aggiornamenti periodici del presente documento, esaminando, in particolare, le revisioni da apportare in base agli aggiornamenti organizzativi interni, alle modifiche della normativa esterna e alle best practice.

Utilizzando un approccio basato sul rischio, su base periodica la Funzione Compliance di Gruppo e il Dipartimento Internal Audit possono svolgere, rispettivamente, attività di monitoraggio o di audit volte a verificare la corretta applicazione della presente Policy all'interno dell'organizzazione.

9. DOCUMENTI CORRELATI

Le seguenti procedure sono correlate alla presente Policy e forniscono dettagli su come la Società intende conformarsi ai requisiti del GDPR. Esse devono essere consultate da tutti i dipendenti di Prysmian per ulteriori indicazioni. Parte di tali documenti sono disponibili nella Sezione Ethics & Integrity del nostro **Intranet aziendale** e sono anche pubblicate nella corrispondente Sezione del nostro **sito web aziendale**.

a) Procedura sulla Data Protection by Design e DPIA;
b) Procedura sui diritti degli interessati;
c) Procedura sulla gestione dei fornitori;
d) Procedura sulla gestione degli incidenti e delle violazioni di dati personali;
e) Procedura sull'uso degli strumenti IT aziendali e poteri di controllo del datore di lavoro;
f) Procedura sulla gestione degli Amministratori di Sistema.

APPENDICE A - DEFINIZIONI

Termini	Significato
Dati personali	Qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"), anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
Trattamento	Qualsiasi operazione o insieme di operazioni compiute su dati personali o serie di dati personali, anche con mezzi automatizzati, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
Soggetto interessato	La persona fisica identificata o identificabile, direttamente o indirettamente, dai dati personali e comunque a cui si riferiscono i dati trattati.
Responsabile del trattamento (o "Responsabile")	La persona fisica o giuridica (ad esempio, outsourcer, fornitori di servizi, consulenti, distributori e agenti), l'autorità pubblica, l'agenzia o altro organismo che tratta i dati personali per conto del Titolare.
Titolare del trattamento (o "Titolare")	Si intende la persona fisica o giuridica, l'autorità pubblica, l'agenzia o altro organismo che, da solo o insieme ad altri, determina le finalità e i mezzi del trattamento dei dati personali, anche per quanto riguarda gli aspetti di sicurezza.
Incaricati del trattamento	Le persone fisiche, come i dipendenti o il personale, che il titolare o il responsabile del trattamento ha autorizzato per iscritto a effettuare operazioni di trattamento dei dati personali.
Il Responsabile della protezione dei dati (o "DPO")	Il soggetto designato dal titolare o dal responsabile del trattamento per svolgere funzioni di supporto e controllo, consultive, formative e informative in relazione all'applicazione del Regolamento stesso. Collabora con l'Autorità

	e costituisce il punto di contatto, anche nei confronti degli Interessati, per le questioni connesse al trattamento dei dati personali.
Internal Data Supervisor (o "IDS")	La persona responsabile di supportare la direzione locale nel definire il corretto "tone at the top" della propria organizzazione aziendale, al fine di garantire la conformità ai requisiti privacy del Gruppo e locali; questa figura implementa e gestisce il Global Privacy Program a livello locale, mantenendo le procedure e i controlli di compliance quotidiani.
Data Owner	Il responsabile di un'area/reparto che tratta dati personali, in grado didelegare l'adempimento dei compiti in materia privacy a uno o più membri del suo team. Nonostante la possibilità di delegare, il Data Owner dei dati rimane pienamente responsabile dei compiti e delle responsabilità assegnati dalla policy in questione.
Privacy Focal Point	Il Privacy Focal Point è un ruolo che può essere definito in Prysmian come punto di contatto locale per il DPO di Gruppo. Se nominato, aiuta il DPO Gruppo a monitorare la conformità alla privacy a livello locale.
Terza parte	La persona fisica o giuridica diversa dall'interessato, dal titolare, dal responsabile e dagli incaricati del trattamento
Consenso	Qualsiasi dichiarazione o azione con cui un interessato manifesta liberamente, specificamente e in modo informato e inequivocabile il proprio consenso al trattamento dei dati personali che lo riguardano.
Violazione dei dati personali	Qualsiasi violazione della sicurezza che comporti la distruzione accidentale o illegale, la perdita, l'alterazione o la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o altrimenti trattati.

APPENDICE B - PRINCIPI GENERALI

Al fine di tutelare i diritti degli interessati, tutti i dati personali devono essere trattati in conformità ai seguenti principi:

- correttezza e trasparenza: i dati sono trattati in modo corretto e trasparente per l'interessato; in particolare, l'interessato deve ricevere un preavviso sufficiente prima di effettuare qualsiasi trattamento ed essere costantemente aggiornato su eventuali modifiche rispetto a quanto inizialmente indicato.
- legittimità: i dati sono raccolti e trattati, ad eccezione delle situazioni obbligatorie espressamente previste dal GDPR, solo se sono soddisfatte una o più condizioni di legittimità definite dal GDPR.
- limitazione delle finalità: i dati vengono raccolti solo per finalità specifiche, esplicite e legittime e non vengono ulteriormente trattati in modo incompatibile con tali finalità.
- minimizzazione dei dati: i dati sono adeguati, pertinenti e limitati a quanto strettamente necessario in relazione alle finalità per cui sono raccolti.
- accuratezza: i dati sono precisi e, ove necessario, aggiornati. Per questo motivo, è necessario adottare tutte le misure necessarie per garantire che i dati inesatti, in relazione alle finalità per cui sono trattati, siano cancellati o rettificati senza indugio.
- limitazione della conservazione: i dati sono conservati in una forma che consenta l'identificazione degli interessati per un periodo non superiore a quello necessario al conseguimento delle finalità per le quali sono stati raccolti e trattati.
- integrità e riservatezza: i dati sono trattati in modo da garantire, mediante l'applicazione di adeguate misure tecniche e organizzative, un adeguato livello di sicurezza, in particolare in termini di protezione contro il trattamento, l'accesso, la distruzione, la perdita, la modifica o la divulgazione non autorizzata dei dati.
- accountability: il titolare del trattamento deve essere in grado di dimostrare che sono state adottate misure e processi adeguati per garantire il rispetto dei principi di cui ai punti precedenti e delle disposizioni del GDPR.