Privacy Policy

Indice delle revisioni

Rev.	Data	Motivo	Pagina
01	15/06/2025	Inserimento figura DPO	Tutte

Sommario

1. Obiettivo e ambito di applicazione

La presente privacy policy (di seguito anche la "**Policy**") si propone di definire ruoli, responsabilità, procedure operative e principi di condotta in materia di gestione dei Dati Personali che Mare Group Spa (" **Mare Group**" ovvero anche la "**Società**") e tutte le società controllate (insieme a Mare Group le "Società"), devono rispettare.

Nel contesto delineato, l'obiettivo principale è definire un metodo uniforme per la gestione dei Dati Personali che garantisca che il Trattamento dei Dati Personali sia conforme alla Direttiva UE n. 679/2016 Regolamento Generale sulla Protezione dei Dati (GDPR) e/o alle leggi e ai regolamenti applicabili.

2. Riferimenti normativi

- Direttiva UE 679/2016 Regolamento Generale per la Protezione dei Dati ("GDPR" o il" Regolamento") che sostituisce la precedente Direttiva UE n. 95/46/CE;
- Decreto 30 giugno 2003, n. 196 e s.m.i. - Codice per la protezione dei dati Personali;
- D.lgs 10 agosto 2018, n.101 e ss.mm.ii. - Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento Europeo;
- D.Lgs 231/2001 - Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di Personalità giuridica.

3. Definizioni generali

Titolare del Trattamento (anche solo "Titolare"):
La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di Dati Personali.

Trattamento/i:
Qualsiasi operazione e insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati applicate a Dati Personali o insiemi di essi, 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.

Responsabile del Trattamento (anche solo il "Responsabile"):
La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta Dati Personali per conto del Titolare del Trattamento.

DPO/RPD: Responsabile Protezione Dati:
La persona fisica che ha la responsabilità di osservare, valutare e organizzare la gestione del trattamento di dati personali (e dunque la loro protezione) all'interno dell'azienda, affinché questi siano trattati nel rispetto delle normative privacy europee e nazionali.

Dati Personali/Dati; Interessato/Interessati:
Qualsiasi informazione riguardante una persona fisica identificata o identificabile ("l'Interessato"/gli "Interessati"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Dati Personali particolari:
Dati Personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale nonché Dati genetici, Dati biometrici intesi a identificare in modo univoco una persona fisica, Dati relativi alla salute o alla vita sessuale ovvero all'orientamento sessuale della persona.

Dati giudiziari
Dati Personali relativi a condanne penali, a reati o a connesse misure di sicurezza, ivi inclusi i dati relativi all'applicazione di misure di prevenzione a seguito di provvedimento giudiziario.

Profilazione:
Qualsiasi forma di Trattamento automatizzato di Dati Personali consistente nell'utilizzo di tali Dati Personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detti persona fisica.

4. Ruoli e responsabilità in ambito privacy

Di seguito sono delineate le figure che fanno parte del modello organizzativo privacy applicabile alle Società:

4.1. Titolare del Trattamento

Il Titolare del trattamento dei Dati Personali è ciascuna Società che, in aderenza alla normativa applicabile, esercita un potere decisionale autonomo sulle finalità e sulle modalità del Trattamento, ivi compreso il profilo sulla sicurezza.
Il Titolare del Trattamento, nella figura del suo Rappresentante Legale:

- è responsabile per le misure tecniche e organizzative poste in essere per garantire che i Trattamenti dei Dati Personali siano effettuati conformemente al GDPR, alla normativa applicabile ed alle regole privacy applicabili;
- sottoscrive la nomina dei fornitori quali Responsabili del Trattamento;
- sottoscrive il Registro delle a5ttività di Trattamento e le sue modifiche sostanziali;
- vigila sul rispetto da parte dei Responsabili del Trattamento delle istruzioni impartite e delle disposizioni vigenti in materia di privacy;
- sottoscrive, ove necessario, l'accettazione della designazione della società quale Responsabile del Trattamento da parte di altri Titolari;
- autorizza nuovi Trattamenti resi necessari per l'operatività della Società;
- garantisce l'informazione e la formazione sulle tematiche relative alla protezione dei dati Personali e sulle regole privacy impartite;
- sottoscrive (i) le comunicazioni al Garante per la Protezione dei Dati Personali o ad altre autorità di controllo, (ii) le risposte alle richieste provenienti dal Garante per la Protezione dei Dati Personali o da altre Autorità di Controllo;
- sottoscrive gli accordi di contitolarità.

4.2. Privacy Manager

Ogni Società deve identificare un Privacy Manager che ha il compito di:

- facilitare, attraverso la propria attività di supporto ai Responsabili di Dipartimento e alle persone autorizzate, l'attuazione e l'applicazione delle regole privacy, inclusa l'attribuzione delle responsabilità, garantendo il rispetto del GDPR e della normativa vigente;
- occuparsi della tenuta e dell'aggiornamento del Registro delle attività di Trattamento per conto di ogni Società, quale Titolare del Trattamento o quale Responsabile del Trattamento per titolari terzi, dietro indicazioni ricevute dai Responsabili di Dipartimento;
- fornire, se richiesto, supporto ai Responsabili di Dipartimento in merito alla Valutazione d'impatto sulla protezione dei dati (DPIA) e sorvegliare i relativi adempimenti;
- supportare i Responsabili di Dipartimento nella gestione degli aspetti legati ai diritti degli Interessati in merito a eventuali richieste connesse al Trattamento dei Dati o all'esercizio dei diritti;
- riportare, con periodicità almeno annuale, all'organismo di vigilanza di ogni Società, ove nominato, l'elenco dei principali eventi in ambito privacy che hanno interessato la Società medesima.

4.3. Responsabile di Dipartimento

Ogni Responsabile di Dipartimento di ciascuna delle Società ha il dovere di promuovere all'interno della propria struttura l'adozione di prassi conformi al GDPR e in linea con la Policy, organizzando e conducendo le attività di competenza in modo da garantire adeguati requisiti di correttezza e sicurezza dei Trattamenti effettuati.
In particolare, ogni Responsabile di Dipartimento deve:

- assicurare che il Trattamento dei Dati Personali avvenga in conformità alle disposizioni di legge

applicabili, nonché nel rispetto dei principi menzionati al successivo paragrafo 5);

- far rispettare le misure di sicurezza tecniche ed organizzative adottate;
- adottare le misure tecniche ed organizzative che si dovessero rendere necessarie per l'applicazione ed il pieno rispetto delle norme emanate in materia di protezione dei Dati Personali, in particolare, al fine di evitare (i) distruzione o perdita, anche accidentale, dei Dati stessi; (ii) accesso non autorizzato; (iii) modifica non autorizzata o impropria dei Dati Personali; (iv) Trattamento non consentito o non conforme alle finalità della raccolta;
- individuare i Trattamenti di pertinenza della propria area aziendale e compilare – tramite il Privacy Manager - il Registro delle attività di Trattamento per la propria area di competenza;
- eseguire la valutazione preliminare dei rischi ed eventuale valutazione dell'impatto prima di procedere con un nuovo Trattamento. Il Responsabile di Dipartimento può chiedere supporto del Privacy Manager in merito allo svolgimento della valutazione o ai relativi esiti;
- in caso di cambiamenti che possano impattare sulle informative verso gli Interessati, apportare le relative modifiche alle informative già emanate e inviarle agli interessati stessi per aggiornamento;
- predisporre il documento di richiesta di consenso per gli specifici Trattamenti della propria direzione e occuparsi della relativa conservazione;
- prestare la propria collaborazione in merito alle richieste inerenti ai Trattamenti svolti sotto la propria responsabilità, avanzate dal Garante per la Protezione dei Dati Personali e/o dall'Autorità Giudiziaria, al fine di consentire all'area competente di fornire le informazioni necessarie;
- fornire la necessaria collaborazione al fine di consentire l'evasione delle istanze degli Interessati nell'esercizio dei diritti previsti dal GDPR, nel rispetto delle tempistiche previste;
- curare che gli eventuali accordi di servizio/collaborazione con soggetti terzi stipulati per le necessità del proprio ambito di competenza siano muniti di clausola privacy che disciplini il Trattamento dei Dati Personali ed il ruolo ad essi assegnato (Titolare autonomo o Responsabile);
- assegnare alle persone autorizzate al Trattamento della propria area specifici compiti ed autorizzazioni necessarie per l'eventuale Trattamento di dati Personali;
- proporre al Titolare, ove ricorrano i presupposti, in caso di accordi di servizio/collaborazione con soggetti terzi, l'attribuzione dell'incarico di Responsabile;
- presidiare l'attività dei Responsabili al Trattamento di competenza;
- ricevere e valutare le comunicazioni dei Responsabili in merito alla sostituzione o designazione di un sub-Responsabile:
- rilevare e segnalare tempestivamente comportamenti in violazione dei principi e delle regole sancite in materia di Trattamento dei Dati Personali.

4.4. Persone autorizzate al trattamento

Le persone Autorizzate al Trattamento sono le persone fisiche che effettuano materialmente le operazioni di Trattamento dei Dati Personali e operano sotto la diretta responsabilità dei Responsabili di Dipartimento e sotto l'autorità del Titolare, attenendosi alle istruzioni impartite.
Si segnala che ciascun dipendente delle Società, coinvolto in attività di Trattamento dei Dati Personali è persona Autorizzata al Trattamento.
Le persone Autorizzate al Trattamento, ad integrazione di quanto previsto nella relativa nomina, trattano i Dati necessari per lo svolgimento delle attività ad essi assegnate nell'ambito delle attribuzioni proprie dell'area aziendale di appartenenza, compiendo le sole operazioni di Trattamento a ciò strumentali, nel rispetto delle regole previste nell'atto di nomina nonché di quelle di seguito descritte. Le persone Autorizzate al Trattamento, nel trattare i Dati Personali, devono operare garantendo la massima riservatezza delle informazioni di cui vengono in possesso, considerando tutti i Dati Personali confidenziali e, di norma, soggetti al segreto professionale.
I Dati Personali non possono essere comunicati a terzi – salvo che per ragioni strettamente connesse all'attività professionale - se non espressamente previsto dalle procedure aziendali e/o se non dietro espressa autorizzazione del Responsabili di Dipartimento.
Le persone Autorizzate al Trattamento devono, inoltre:

- operare con la massima diligenza ed attenzione in tutte le fasi di Trattamento dei Dati, dalla loro esatta acquisizione all'eventuale aggiornamento;

- assicurare la custodia dei Dati ed eseguire operazioni di cancellazione o distruzione solo nei casi previsti;
- non eseguire operazioni di Trattamento per fini non previsti tra i compiti loro assegnati dai diretti responsabili o superiori e, comunque, non in linea alle disposizioni e regolamenti vigenti;
- evitare che i Dati Personali siano soggetti a rischi di distruzione e/o perdita anche accidentale;
- evitare che ai Dati possano accedere persone non autorizzate;
- evitare che vengano svolte operazioni di trattamento non consentite e/o non conformi alle finalità per cui i Dati sono stati raccolti;
- evitare di iniziare nuovi Trattamenti se non espressamente autorizzati;
- evitare di effettuare copie di archivi di Dati Personali, anche parziali, a meno che non espressamente richiesto per l'esecuzione delle proprie mansioni.

Le persone Autorizzate al Trattamento che svolgono eventualmente Trattamenti di Dati particolari potranno ricevere ulteriori specifiche indicazioni scritte a cura del Responsabile di Dipartimento ad integrazione di quelle generali di cui al presente documento e ad integrazione delle indicazioni contenute nell'atto di nomina.

4.5. Responsabile del trattamento

Il Responsabile del Trattamento è il soggetto che effettua Trattamenti per conto del Titolare.
In presenza di un Responsabile del Trattamento i Dati Personali permangono comunque nell'ambito di ogni Società che rimane Titolare del Trattamento non solo dei propri Trattamenti ma anche di quelli posti in essere dal soggetto terzo designato Responsabile.
I Trattamenti eseguiti dal Responsabile del Trattamento sono disciplinati nell'ambito di un contratto o altro atto giuridico, e censiti nell'apposito documento, che indica altresì, tra l'altro, l'ambito, la durata, la natura e la finalità del Trattamento, il tipo di Dati Personali e le categorie di Interessati. I compiti affidati ai Responsabili del Trattamento sono pure contemplati nel predetto apposito documento, i cui contenuti sono definiti dal Titolare che, con il supporto dei Responsabili di Dipartimento e del Privacy Manager ne cura il relativo aggiornamento derivante da variazioni normative e/o operative.

Nomina del Responsabile

In caso di instaurazione di un rapporto di servizio/collaborazione, al fine di assicurare il corretto inquadramento del soggetto terzo e la gestione della privacy nell'ambito di detto rapporto, il Responsabile di Dipartimento identifica e valuta, confrontandosi con il Titolare, se necessario, i sottostanti Trattamenti di Dati Personali, accerta l'eventuale tipologia di Trattamento e verifica l'effettiva ripartizione dei compiti tra le parti in relazione alla gestione del Trattamento.
Nel caso in cui ricorrono i presupposti per designare il soggetto terzo come Responsabile del Trattamento, i Responsabili di Dipartimento dovranno:

- confrontarsi con il Privacy Manager per verificare l'effettiva necessità della nomina;
- proporne la nomina al Titolare, mediante sottoscrizione dell'apposito "Atto di nomina";
- trasmettere l'atto di nomina al soggetto terzo richiedendo la sottoscrizione per accettazione dell'incarico con indicazione della data sulla copia della lettera stessa;

Il Responsabile di Dipartimento, in luogo del Titolare, conserva l'Atto di nomina a Responsabile del Trattamento sottoscritto per accettazione, presso la propria struttura, anche per eventuali ispezioni del Garante per la Protezione dei Dati Personali ed effettua l'aggiornamento dell'elenco dei suoi responsabili, che invia al Privacy Manager per la tenuta complessiva della lista dei Responsabili.
Il Responsabile del Trattamento deve fornire adeguate garanzie in merito all'adozione di misure tecniche ed organizzative adeguate a garantire la protezione dei diritti dell'Interessato.

4.6. Amministratore di sistema

Con la definizione di Amministratore di Sistema (di seguito anche "ADS") si individuano, in ambito informatico, le figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. A questi vengono equiparate, dal punto di vista dei rischi relativi alla protezione dei Dati, anche altre figure, quali gli amministratori di basi di Dati, gli amministratori di reti e di apparati di sicurezza e gli

amministratori di sistemi software complessi.
Gli Amministratori di Sistema come sopra individuati nelle loro consuete attività sono concretamente "responsabili" di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei Dati. Attività tecniche quali il salvataggio dei Dati (c.d. funzioni di *Backup* e *Recovery*), l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione *hardware* comportano, infatti, un'effettiva capacità di azione su informazioni e dati che va considerata a tutti gli effetti come un Trattamento di Dati Personali.
Il Garante per la Protezione dei Dati personali, pertanto, ha prescritto ai Titolari del Trattamento l'adozione di accorgimenti e misure volte a garantire la sicurezza dei Dati Personali in relazione alla particolare criticità del ruolo dell'Amministratore di Sistema, insita nella sua capacità di accedere in modo esclusivo e privilegiato alle risorse del sistema informativo aziendale.
Per effetto di tale disposizione, l'attribuzione delle funzioni di Amministratore di Sistema deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di Trattamento ivi compreso il profilo relativo alla sicurezza. Le nomine di ADS sono conservate dal dipartimento Risorse Umane.

Le figure sopra esposte afferiscono al **Dipartimento Information Technology** che ha il compito di implementare misure di sicurezza appropriate a livello tecnologico e infrastrutturale. Il dipartimento, con gli ADS, supporta il Titolare e il Privacy Manager nella gestione di violazioni dei dati ("data breach").

4.7. Data Protection Officer /Responsabile della Protezione Dati (DPO/RPD)

Il data Protection Officer (di seguito DPO) è una figura introdotta dal Regolamento generale sulla protezione dei dati 2016/679 | GDPR, pubblicato sulla Gazzetta Ufficiale europea L. 119 il 4 maggio '16.
Il DPO, figura storicamente già presente in alcune legislazioni europee, è un professionista che deve avere un ruolo aziendale (sia esso soggetto interno o esterno) con competenze giuridiche, informatiche, di risk management e di analisi dei processi. La sua responsabilità principale è quella di osservare, valutare e organizzare la gestione del trattamento di dati personali (e dunque la loro protezione) all'interno di un'azienda (sia essa pubblica che privata), affinché questi siano trattati nel rispetto delle normative privacy europee e nazionali.
L'art. 39 del Regolamento europeo sulla protezione dei dati personali elenca i principali compiti del DPO (Responsabile della protezione dei dati):
1. Il responsabile della protezione dei dati | DPO | è incaricato almeno dei seguenti compiti:
a) informare e fornire consulenza al Titolare del trattamento o al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento Privacy UE 2016/679 (GDPR), nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

b) sorvegliare l'osservanza del Regolamento Privacy UE 2016/679 (GDPR), di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del Titolare del trattamento o del Responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;
d) cooperare con l'autorità di controllo;
e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

2. Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

5. Principi in materia di Trattamento dei Dati Personali

I Dati Personali vengono:

- raccolti per finalità specifiche, chiare e lecite e quindi trattati limitatamente a tali finalità;

- conservati in modo da garantirne la correttezza;
- aggiornati, adottando tutte le misure ragionevoli per cancellare o modificare con tempestività dati inesatti in riferimento alle finalità pertinenti;
- archiviati per un periodo che non dovrà superare i tempi previsti di conservazione degli stessi.

I Dati Personali devono essere trattati in modo da garantirne la sicurezza mediante l'adozione di adeguate misure tecniche e organizzative.

6. Diritti degli Interessati

Di seguito vengono descritti i principali requisiti da soddisfare in riferimento all'esercizio dei diritti dei soggetti Interessati.

6.1. Diritto all'Informativa

A) Informativa qualora i Dati siano raccolti presso l'Interessato
In caso di raccolta presso l'Interessato di Dati Personali che lo riguardino (Informativa "diretta"), il Titolare del Trattamento fornisce allo stesso, nel momento in cui i Dati sono ottenuti, informazioni riguardanti l'identità e i Dati di contatto del Titolare stesso, le finalità del Trattamento cui sono destinati i Dati Personali, nonché la base giuridica del Trattamento stesso. Vengono altresì fornite informazioni necessarie a garantire un Trattamento corretto e trasparente nei confronti dell'Interessato inerenti il periodo di conservazione indicato dei Dati Personali ovvero i criteri utilizzati per stabilire tale periodo. Viene specificato, inoltre, che l'Interessato ha il diritto di richiedere al Titolare l'accesso ai Dati Personali, di rettificarli e cancellarli, di limitare il Trattamento od opporsi allo stesso, in aggiunta al diritto alla portabilità dei Dati e al diritto di revocare il consenso in qualsiasi momento, senza pregiudicare la liceità del Trattamento basata sul consenso prima della revoca.
Queste informazioni vengono fornite all'Interessato per iscritto, in formato elettronico o cartaceo, ovvero oralmente se ciò è richiesto dall'Interessato di cui sia comprovata l'identità. Successivamente vengono riformulate e integrate, qualora il Titolare del Trattamento intenda continuare a trattare i Dati Personali per finalità diverse da quelle per le quali i Dati erano stati raccolti.

B) Informativa qualora i Dati non siano stati ottenuti presso l'Interessato
Se i Dati non sono stati ottenuti presso l'Interessato, il contenuto dell'Informativa che il Titolare del Trattamento fornisce all'Interessato è sostanzialmente il medesimo di quella "diretta", con l'aggiunta, tuttavia, di alcune indicazioni che non sarebbero altrimenti conoscibili all'Interessato, relative alla fonte dalla quale provengono i Dati Personali e, se del caso, all'eventualità che i Dati provengano da fonti accessibili al pubblico, nonché alle categorie di Dati trattati.

6.2. Diritto di accesso dell'interessato

L'Interessato ha il diritto di ottenere dal Titolare del Trattamento la conferma che sia o meno in corso un Trattamento di Dati Personali che lo riguarda e, in tal caso, di ottenere l'accesso ai Dati Personali e ad alcune informazioni riguardanti:

- Le finalità del Trattamento;
- Le categorie di Dati Personali trattati;
- I destinatari o le categorie di destinatari a cui i Dati Personali sono stati o saranno comunicati, in particolare se i destinatari sono ubicati in paesi terzi o sono organizzazioni internazionali;
- Se possibile, il periodo di conservazione dei Dati Personali forniti o, in alternativa, i criteri utilizzati per determinare tale periodo;
- L'esistenza del diritto dell'Interessato di chiedere al Titolare del trattamento la rettifica o la cancellazione dei Dati Personali o la limitazione del Trattamento dei Dati Personali che lo riguardano o di opporsi al loro Trattamento;
- Il diritto a presentare reclamo presso un'autorità di controllo;
- Se i Dati non sono stati raccolti presso l'Interessato, tutte le informazioni disponibili sulla loro origine;
- L'esistenza di un processo decisionale automatizzato, compresa la Profilazione, e, almeno in tali casi,

informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale Trattamento per l'Interessato.

6.3. Diritto di rettifica dei dati e diritto all'oblio

L'Interessato ha il diritto di chiedere al Titolare del Trattamento la rettifica di Dati Personali inesatti che lo riguardano senza ingiustificato ritardo, nonché di ottenerne l'integrazione qualora siano incompleti, anche attraverso una dichiarazione integrativa.
L'Interessato ha altresì il diritto di chiedere al Titolare del Trattamento la cancellazione dei Dati Personali ("diritto all'oblio") senza ingiustificato ritardo, ad esempio, se i Dati non sono più necessari rispetto alle finalità per le quali sono stati raccolti, se l'Interessato ha revocato il consenso o ha esercitato il diritto a opporsi al Trattamento, se i Dati Personali sono stati trattati illecitamente, ecc. Il Titolare del Trattamento ha l'obbligo di procedere alla cancellazione senza ingiustificato ritardo. Inoltre, se i Dati sono stati comunicati a terzi o resi pubblici, la richiesta dell'Interessato viene trasmessa, da parte del Titolare, a tali soggetti.
Sono previsti dei limiti al diritto alla cancellazione, nella misura in cui il Trattamento sia necessario per l'esercizio del diritto alla libertà di espressione o di informazione, per l'adempimento di un obbligo legale, per motivi di interesse pubblico ovvero per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

6.4. Diritto di limitazione del trattamento dei dati

A richiesta dell'Interessato, è possibile ottenere una limitazione del Trattamento dei Dati, laddove l'Interessato contesti l'esattezza dei Dati Personali, per il periodo necessario al Titolare per verificare l'esattezza di tali Dati o si opponga al Trattamento degli stessi, o quando i Dati Personali siano necessari all'Interessato per accertare, esercitare o difendere un diritto in sede giudiziaria benché il Titolare non abbia più bisogno di tali Dati per il Trattamento, ovvero quando il Trattamento è illecito né l'Interessato si oppone alla cancellazione dei Dati e chiede, invece, che ne sia limitato l'utilizzo.

6.5. Diritto alla portabilità dei dati

E' riconosciuta all'Interessato la possibilità di chiedere al Titolare che tratta i suoi dati di restituire gli sessi, nonché quella di trasmettere i Dati ad altro Titolare a condizione che il Trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b) GDPR e venga effettuato mediante mezzi automatizzati.

6.6. Diritto di opposizione

L'Interessato può opporsi al Trattamento dei propri Dati Personali per tre ordini di motivi:
- Per ragioni connesse alla sua particolare situazione, nei casi di Trattamento per scopi di interesse pubblico o per legittimo interesse, ivi compresa la profilazione. Il Titolare deve astenersi dal trattare ulteriormente detti Dati, salvo che dimostri la sussistenza di motivi legittimi cogenti per procedere al Trattamento;
- Qualora i Dati Personali siano trattati per finalità di marketing diretto. In tal caso l'Interessato può opporsi in ogni momento al Trattamento dei propri Dati, di talché dopo l'opposizione non sarà più possibile trattarli per fini commerciali;
- Qualora i Dati Personali siano trattati a fini di ricerca scientifica o storica ovvero a fini statistici. In questi casi il diritto dell'Interessato può essere limitato solo nell'ipotesi in cui il Trattamento sia necessario per l'esecuzione di un compito di interesse pubblico.

6.7. Diritto a non essere sottoposti a processi decisionali automatizzati

L'Interessato ha il diritto di opporsi a una decisione basata unicamente sul Trattamento automatizzato, inclusa la profilazione, nella misura in cui tali attività di Trattamento possono produrre effetti giuridici che lo riguardano o incidere in modo analogo significativamente sulla sua persona. Per processo decisionale automatizzato si deve pertanto intendere una decisione presa sulla sola base di Dati Personali artificialmente generati mediante algoritmi (come ad es. fattori di calcolo matematici e processi statistici), applicati a un insieme di Dati Personali di partenza riconducibili all'Interessato, senza il coinvolgimento di un essere umano che possa influenzare ed eventualmente cambiare il risultato attraverso la sua autorità o competenza.
Il diritto in questione è derogabile soltanto consensualmente, in seguito ad accordo contrattuale che renda

necessaria una decisione esclusivamente basata su algoritmi o in base a consenso esplicito al Trattamento espresso dall'Interessato, ovvero per disposizione di legge, laddove la decisione sia autorizzata dal diritto interno o da quello dell'UE.

6.8. Richieste degli interessati

Gli Interessati possono presentare richieste riguardanti l'esercizio dei loro diritti utilizzando l'indirizzo della sede legale di ogni Società ovvero l'indirizzo e-mail/pec indicato in ogni informativa. Ogni Società evaderà la richiesta e fornirà agli Interessati tutte le informazioni necessarie in forma comprensibile, concisa, accessibile e attraverso l'utilizzo di un linguaggio semplice e chiaro.
Si veda in merito la "Procedura in materia di gestione dei diritti dell'Interessato".

7. Trattamento di categorie particolari di Dati Personali

Il Regolamento individua determinate tipologie di Dati il cui Trattamento potrebbe porre rischi significativi per i diritti e le libertà fondamentali. Nelle categorie particolari di Dati Personali rientrano tutti i Dati che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, nonché il Trattamento di Dati genetici, Dati biometrici intesi a identificare in modo univoco una persona fisica, Dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Il Trattamento di tutte le predette tipologie di Dati è possibile esclusivamente nei seguenti casi:
- l'Interessato ha prestato il proprio consenso esplicito al Trattamento di tali Dati Personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'Interessato non possa revocare il divieto;
- il Trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del Titolare del Trattamento o dell'Interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'Interessato;
- Il Trattamento è necessario per tutelare un interesse vitale dell'Interessato o di un'altra persona fisica qualora l'Interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
- Il Trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria od ogniqualvolta le autorità giudiziarie esercitino le loro funzioni giurisdizionali;
- Il Trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei Dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'Interessato;
- Il Trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione e degli Stati membri o conformemente al contratto con un professionista della sanità.

8. Registro delle attività di Trattamento

Ogni Società è obbligata a predisporre e tenere il Registro delle attività di Trattamento.
Ogni Responsabile di Dipartimento di ognuna delle Società è responsabile del Trattamento dei Dati Personali afferenti la propria area e deve tempestivamente comunicare, al Privacy Manager – che è responsabile dell'aggiornamento del registro delle attività di Trattamento secondo le indicazioni ricevute da ogni Responsabile di Dipartimento - nuovi o modificati Trattamenti esistenti (ad esempio, modifiche o integrazioni a categorie di Dati Personali trattati, definizione di nuove finalità di Trattamento da inserire in comunicazioni, condizioni contrattuali con soggetti terzi, ecc.). Indipendentemente dalle comunicazioni di ogni singola funzione, il Privacy Manager rivede annualmente il Registro.
Il Registro deve essere messo a disposizione dell'Autorità di controllo.

9. Misure di sicurezza per il trattamento dei dati

Al fine di garantire un livello di sicurezza adeguato al rischio, le Società hanno l'obbligo di definire e mettere in atto misure tecniche e organizzative, tenendo conto dello stato dell'arte e dei costi di attuazione in riferimento ai rischi associati al Trattamento e alla natura dei Dati Personali da proteggere, secondo i principi della "privacy by design" (fin dalla progettazione) e della "privacy by default".
Devono essere considerati i rischi presentati dal Trattamento che derivano nello specifico da distruzione, perdita, modifica non autorizzati, ecc.; ogni Responsabile di Dipartimento, eventualmente con il supporto del Privacy Manager ovvero del Responsabile IT definisce ed adotta le misure di sicurezza che possono garantire un adeguato livello di protezione dei Dati Personali di default e anche preventivamente in relazione al Trattamento dei Dati Personali.

10. Valutazione d'impatto sulla protezione dei dati

Al fine di assicurare un livello adeguato di protezione dei Dati, è necessario adottare misure tecniche e organizzative che garantiscano una protezione commisurata al livello di sicurezza stabilito in base ai rischi per i diritti e le libertà degli Interessati.
A tal fine, per ogni attività di Trattamento identificata nel Registro che può comportare un rischio elevato per i diritti e le libertà degli Interessati, ogni Responsabile di Dipartimento di ognuna delle Società esegue una valutazione dell'impatto sulla protezione dei Dati (Valutazione dell'Impatto sulla Protezione dei Dati, di seguito anche "DPIA").
A prescindere dai livelli di rischio risultanti, il DPIA è richiesto in tutti i casi in cui vi sia:

- La valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un Trattamento automatizzato, compresa la Profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
- Il Trattamento, su larga scala, di categorie particolari di Dati Personali o di Dati Personali relativi a condanne penali e reati;
- La sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Il DPIA certifica che il Titolare ha valutato in modo adeguato i possibili rischi e ha adottato misure di protezione adeguate.
Per il contenuto del DPIA si rimanda all'apposita procedura.

11. Gestione e notifica di violazione dei dati personali

In caso di una violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata dei dati che ne comprometta la riservatezza, la disponibilità o l'integrità, previo coinvolgimento del Privacy Manager, del Responsabile di Dipartimento coinvolto, del Responsabile Dipartimento IT /(ADS) e del DPO quando la violazione coinvolge i sistemi informatici, il Titolare del Trattamento ha l'obbligo di notificare tale violazione al Garante per la Protezione dei Dati Personali entro 72 ore dal momento in cui ne è venuto a conoscenza e deve:

- descrivere la natura della violazione dei Dati, compresi, ove possibile, le categorie e il numero approssimativo di Interessati;
- comunicare i dati di contatto della società coinvolta;
- descrivere le probabili conseguenze della violazione dei Dati verificatasi;
- descrivere le misure adottate o di cui si propone l'adozione da parte del Titolare del Trattamento per porre rimedio alla violazione dei Dati Personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Qualora la notifica non sia stata effettuata entro 72 ore, è corredata dai motivi del ritardo.
Nei casi in cui la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, previa consultazione con il Privacy Manager, il Titolare del Trattamento comunica la violazione all'Interessato senza ingiustificato ritardo. Tale comunicazione non è richiesta se il Titolare del Trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione o se tale comunicazione comporterebbe sforzi sproporzionati.
La scelta della modalità di comunicazione deve tenere conto dell'accessibilità degli Interessati in diversi modi e, se del caso, della diversità linguistica dei destinatari.
Qualsiasi violazione dei Dati Personali, presunta o accertata, deve essere adeguatamente registrata e

documentata al fine di garantire il rispetto del principio di responsabilizzazione.
Per ogni approfondimento si rimanda all'apposita procedura.

12. Formazione

A fine di garantire la conformità alla legislazione vigente di tutte le attività di Trattamento dei Dati Personali svolte sotto l'autorità del Titolare del Trattamento da chiunque faccia parte della struttura aziendale e abbia accesso ai Dati Personali, tramite il Dipartimento Risorse Umane, sono organizzate attività di formazione rivolte al personale riguardanti la protezione dei Dati Personali.

13. Gestione delle relazioni con l'Autorità di controllo

In caso di richiesta, ognuna delle Società deve collaborare con l'Autorità di controllo:

- mettendo il Registro delle attività di Trattamento a disposizione dell'Autorità di controllo, su sua richiesta;
- notificando all'Autorità di controllo qualsiasi violazione dei Dati Personali conformemente alle procedure descritte nel precedente paragrafo 11);
- consultando l'Autorità di controllo quando la valutazione d'impatto sulla protezione dei Dati dimostra un rischio elevato di Trattamento, secondo la metodologia di analisi del rischio descritta nella apposita procedura.

14. Efficacia della Policy. Modifiche

La Policy è immediatamente operativa.
Ogni eventuale modifica sarà prontamente comunicata.