

POLITICA PER LA PROTEZIONE DEI DATI PERSONALI

GRUPPO GRIMALDI

Uso Interno

REGISTRO DELLE MODIFICHE

Rev.	Data	Descrizione	Stato	Redazione

Verifica	Approvazione

SOMMARIO

1.	OBIETTIVO	4
1.1	CAMPO DI APPLICAZIONE.....	4
1.2	NORMATIVA DI RIFERIMENTO.....	5
2.	POLITICA PER LA PROTEZIONE DEI DATI PERSONALI	6
3.	I DIRITTI DELL'INTERESSATO.....	14
3.1	ESERCIZIO DEI DIRITTI DELL'INTERESSATO E TEMPI DI RISCONTRO.....	14
3.2	DIRITTO DI ACCESSO AI DATI DA PARTE DELL'INTERESSATO.....	15
3.3	DIRITTO DI RETTIFICA.....	16
3.4	DIRITTO DI CANCELLAZIONE	16
3.5	DIRITTO DI LIMITAZIONE DI TRATTAMENTO	17
3.6	DIRITTO ALLA PORTABILITÀ DEI DATI	17
3.7	DIRITTO DI OPPOSIZIONE	18

1. OBIETTIVO

Obiettivo di questa Politica è rappresentare le regole e i principi cui le Società facenti parte del Gruppo Grimaldi si sono adeguate in ossequio a quanto stabilito:

- dal Regolamento UE n. 679/2016 *Regolamento Generale sulla Protezione dei dati* (di seguito anche “Regolamento”);
- dal Decreto Legislativo n. 196/2003 “*Codice in materia di protezione dei dati personali*” (di seguito “Codice Privacy”), dagli allegati al Codice così come modificati dalla Legge 25 ottobre 2017, n. 163 *Delega al Governo per il recepimento delle direttive europee e l’attuazione di altri atti dell’Unione europea - Legge di delegazione europea 2016-2017*;
- Dai Provvedimenti, dalle Linee Guida e dai Pareri emessi dall’Autorità Garante per la protezione dei dati personali (di seguito “Garante Privacy”), dal GdL ex art. 29¹ e dal Garante Europeo della Protezione dei Dati (GEPD).

Scopo della presente Policy è descrivere l’impegno delle Società facenti parte del Gruppo Grimaldi per:

- proteggere e salvaguardare i dati personali e confidenziali;
- disciplinare il trattamento dei dati personali e confidenziali;
- stabilire i principi di buona gestione per i dati personali e confidenziali;
- garantire che tutti i trattamenti avvengano nel rispetto dei diritti, delle libertà fondamentali nonché della dignità delle persone fisiche;
- assicurare la riservatezza delle informazioni riferite ai clienti e a tutti coloro che hanno rapporti con le singole Società del Gruppo.

1.1 Campo di Applicazione

La Policy si applica a tutti i trattamenti di dati personali, confidenziali, rischiosi, sensibili e giudiziari effettuati a qualsiasi titolo dalle Società del Gruppo Grimaldi (come di seguito meglio identificate) operanti sul territorio nazionale, ciascuna delle quali nel suo ruolo di autonomo Titolare dei trattamenti di dati personali effettuati nel proprio ambito societario ovvero nel loro ruolo di Contitolari per le aree oggetto di apposito accordo, sottoscritto in data 21/05/2018.

Inoltre la presente Policy si applica a tutti i dati personali di persone fisiche (tra cui, a titolo esemplificativo e non esaustivo, quelli afferenti a dati dei dipendenti, dei clienti, dei fornitori e dei soggetti terzi che operano in qualità di persona fisica) nonché a qualsiasi informazione di carattere personale o con le caratteristiche di dato personale ricevute da altre entities del Gruppo (ivi comprese quelle ubicate in altri Stati Membri).

¹ Il Gruppo, istituito dall’art. 29 della Direttiva 95/46, è un organismo consultivo e indipendente, composto da un rappresentante delle autorità di protezione dei dati personali designate da ciascuno Stato membro, dal GEPD (Garante europeo della protezione dei dati), nonché da un rappresentante della Commissione. Il Gruppo di lavoro ex articolo 29, sarà sostituito a partire dal 25 maggio 2018 dal *Comitato europeo per la protezione dei dati*. Il comitato, che sostituirà il WP29, è un elemento vitale della riforma e dovrà essere pienamente operativo sin dal primo giorno

Le legal entity del Gruppo Grimaldi (di seguito, per brevità, denominate cumulativamente come “*Società del Gruppo*”) cui si applicano i contenuti della presente Policy sulla protezione dei dati personali e confidenziali dei clienti (di seguito per brevità “la Policy”) sono:

Grimaldi Group S.p.A.

Gramaldi Euromed S.p.a.

Grimaldi Deep S.p.A.

1.2 Normativa di riferimento

- [1] Regolamento UE n. 679/2016 *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE* (Regolamento Generale sulla protezione dei dati);
- [2] D.Lgs. n. 196/03 *Codice in materia di protezione dei dati personali*;
- [3] Documento WP 243 – *Linee guida sui responsabili della protezione dei dati (RPD) del 13 dicembre 2016*;
- [4] Documento WP 248 rev.01 - *Linee guida in materia di valutazione d’impatto sulla protezione dei dati e determinazione della possibilità che il trattamento “possa presentare un rischio elevato”*
- [5] Documento WP 250 rev.01 - *Guidelines on Personal data breach notification*

2. POLITICA PER LA PROTEZIONE DEI DATI PERSONALI

Le Società appartenenti al Gruppo Grimaldi si impegnano a proteggere i dati personali e confidenziali trattati a qualsiasi titolo adeguando le proprie azioni ai seguenti Principi generali:

A. Raccolta e trattamento delle informazioni

Le Società del Gruppo adottano le misure e le precauzioni per verificare che le informazioni contenenti dati personali siano pertinenti, accurate, complete e attuali come è necessario per gli scopi per i quali devono essere utilizzate.

I trattamenti di dati personali effettuati si conformano al principio di minimizzazione dei dati ai sensi dell'art. 5, co. 1, lett. c), del Regolamento in base al quale la raccolta e il successivo trattamento di dati personali avvengono in maniera da ridurre al minimo indispensabile l'utilizzo di dati personali identificativi degli Interessati.

Qualora alcune operazioni di trattamento, ovvero processi o fasi di processo, non necessitino la visualizzazione in chiaro di dati personali e identificativi degli Interessati, le medesime operazioni di trattamento devono essere effettuate mediante dati resi anonimi o, quantomeno, codificati.

B. Informativa

Le Società del Gruppo si adoperano affinché tutte le operazioni di trattamento avvengano conformemente a quanto richiesto dall'art. 13 del Regolamento.

L'informativa deve essere sempre resa agli interessati all'atto della raccolta dei dati, anche quando non è necessario richiedere il loro consenso al trattamento.

L'informativa rispetta i seguenti principi:

- non è consentito effettuare trattamenti di dati personali senza aver fornito preventivamente l'informativa;
- non è consentito effettuare trattamenti di dati personali per finalità diverse da quelle indicate nell'informativa già resa ai clienti; ulteriori finalità possono essere integrate nell'informativa previa condivisione con i Responsabili del trattamento.
- non è consentita la comunicazione dei dati alle categorie dei soggetti terzi diverse da quelle indicate nell'informativa. Eventuali ulteriori categorie di soggetti ritenute necessarie ai fini del trattamento dei dati possono essere inserite nell'informativa previa condivisione con i Responsabili del trattamento.

Le Società del Gruppo si impegnano affinché sia previsto un aggiornamento periodico e/o una review delle varie informative sia cartacee (i.e. informativa dipendenti, informativa marittimi, informativa passeggeri etc.) sia elettroniche (i.e. informative siti web).

C. Scelta e consenso

Le Società del Gruppo s'impegnano a rispettare l'obbligo di raccolta del consenso come stabilito dagli artt. 6 e 7 del Regolamento.

Il consenso è validamente prestato quando:

- è preceduto da un'informativa corretta e completa;
- è espresso liberamente;
- è riferito univocamente ad un determinato trattamento;
- è documentato per iscritto in relazione al tipo di dati raccolti (ad es. uso di dati sensibili).

Ai sensi dell'art. 6, comma 1, lett. b) – f), del Regolamento il consenso non è dovuto quando:

- il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
- il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
- il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
- il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
- il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

D. Accesso ai dati personali e altri diritti dell'Interessato

Le Società del Gruppo garantiscono a ciascun individuo di cui sono trattati i dati personali il libero esercizio dei diritti previsti dagli artt. 15- 22 del Regolamento.

In particolare l'Interessato ha il diritto di:

- ottenere la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, ottenerne l'accesso;
- opporsi ad un determinato trattamento di dati personali per motivi legittimi al fine di farlo cessare definitivamente;
- revocare il proprio consenso in qualsiasi momento, senza che venga pregiudicata la liceità del trattamento basata sul consenso prima della revoca;
- ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano, senza ingiustificato ritardo e l'integrazione dei dati personali incompleti, anche tramite apposita dichiarazione integrativa;

- richiedere che i propri dati siano trattati unicamente ai fini di conservazione, con esclusione di qualunque altra operazione di trattamento;
- ottenere la cancellazione dei propri dati personali quando ne ricorrano i presupposti.

E. Trasferimento di dati personali

Le Società del Gruppo s'impegnano ad adottare le misure necessarie per garantire che i trasferimenti di dati personali siano conformi con la normativa applicabile anche nel caso in cui questo dovesse avvenire da parte di soggetti terzi che agiscono in qualità di sub-appaltatori.

In ossequio al principio di libera circolazione dei dati personali, il Regolamento regola il trasferimento dei dati tra gli Stati membri dell'Unione Europea o allo Spazio Economico Europeo (Norvegia, Islanda, Liechtenstein).

Per il trasferimento dei dati verso un Paese non appartenente alla UE/SEE, invece, devono sussistere una o più delle seguenti condizioni:

- L'ordinamento del paese di destinazione o di transito dei dati assicura un livello di tutela delle persone giudicato "adeguato" dalla Commissione Europea
- sono stati adottati strumenti contrattuali che offrano garanzie adeguate (*Standard contractual clauses, Binding corporate rules, etc.*);
- l'interessato abbia esplicitamente manifestato il proprio consenso al trasferimento (per iscritto, in caso di dati sensibili) al trasferimento proposto, dopo essere stato informato dei possibili rischi di siffatti trasferimenti per l'interessato, dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate;
- il trasferimento sia necessario all'esecuzione di un contratto concluso tra l'interessato e il titolare del trattamento ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'interessato;
- il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto stipulato tra il titolare del trattamento e un'altra persona fisica o giuridica a favore dell'interessato;
- il trasferimento sia necessario per importanti motivi di interesse pubblico;
- il trasferimento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;
- il trasferimento sia necessario per tutelare gli interessi vitali dell'interessato o di altre persone, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso.

F. Integrità dei dati

Le Società del Gruppo Grimaldi ai sensi dell'art. 5 del Regolamento, effettuano i trattamenti di dati personali adeguando il loro operato ai seguenti criteri generali:

- ciascun trattamento deve avvenire in modo lecito, trasparente e secondo correttezza;

- i dati trattati devono essere raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini non incompatibili con tali scopi;
- i dati trattati devono essere esatti e, se necessario, aggiornati;
- i dati trattati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- i dati trattati devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;
- i dati devono essere trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («*integrità e riservatezza*»).

G. Sicurezza dei dati

Le Società del gruppo Grimaldi s'impegnano ad adottare, nei limiti del possibile, le misure di sicurezza necessarie e adeguate affinché i dati e le informazioni personali siano protetti da perdita, uso improprio, accesso non autorizzato, divulgazione, alterazione o distruzione oltre che le ragionevoli verifiche affinché tali misure risultino costantemente aggiornate.

In base a quanto disposto dagli articoli 24 e 32 del Regolamento tutte le Società del Gruppo Grimaldi hanno varato un programma di sicurezza che prevede l'adozione di misure in linea con i seguenti principi:

- garantire che siano trattati i dati personali per impostazione predefinita necessari per ogni specifica finalità del trattamento (*Security e Privacy by Default*);
- attuare in modo efficace i principi di protezione dei dati e integrare nel trattamento fin dalla progettazione le necessarie garanzie al fine di tutelare i diritti degli interessati (*Security e Privacy by Design*);
- assicurare, in caso di violazione dei dati personali, la comunicazione verso gli interessati e il Garante Privacy nei modi e nei tempi del Regolamento;
- effettuare per quei trattamenti che presentano rischi elevati per i diritti e la libertà degli interessati la valutazione d'impatto nei modi e nei tempi previsti dal Regolamento;
- garantire adeguata formazione specialistica sulle tematiche di sicurezza IT;
- adottare tecniche di anonimizzazione o cifratura dei dati personali quando necessario.

Ciò premesso, e in aggiunta a quanto precede, le Società del Gruppo si impegnano a trattare i dati personali solo qualora sono implementati i seguenti presidi:

- **Sistemi di autenticazione informatica**

Le Società del Gruppo adottano credenziali di autenticazione che consistono in un codice per l'identificazione dell'utente (UserID) associato a una parola chiave riservata conosciuta solamente dal medesimo (password).

Ad ogni utente sono assegnate ed associate individualmente una o più credenziali per l'autenticazione.

- **Segretezza e custodia delle credenziali di autenticazione**

Le Società del Gruppo invitano gli utenti a conservare con la massima riservatezza le proprie credenziali di autenticazione e a non condividerle con altri utenti. Tutti gli utenti sono responsabili del corretto e lecito utilizzo delle di credenziali di autenticazione assegnate.

- **Password**

Le Società del Gruppo utilizzano password composte almeno da un numero pari ad 8 caratteri, e comunque, non inferiore da quello richiesto, volta per volta, per legge e con caratteristiche tali da rendere difficoltoso l'eventuale tentativo di individuazione.

La password è modificata ogni 90 giorni, ovvero con cadenza periodica inferiore (i.e. 30 giorni), in funzione della tipologia di dati trattati (i.e. dati particolari: sensibili, giudiziari, etc.), al fine di ridurre il rischio che utenti non autorizzati o malintenzionati riescano ad individuarla.

Gli utenti devono modificare la propria password al primo accesso e possono modificarla successivamente. Non possono essere riutilizzare le 5 password usate precedentemente.

Le password, non devono contenere il nome account dell'utente o riferimenti agevolmente riconducibili all'utente medesimo e devono contenere caratteri di almeno tre delle quattro categorie seguenti:

- Lettere maiuscole dell'alfabeto latino (dalla A alla Z);
- Lettere minuscole dell'alfabeto latino (dalla a alla z);
- Numeri in base 10 (da 0 a 9);
- Caratteri non alfanumerici, ad esempio punto esclamativo (!), dollaro (\$), simbolo di cancelletto (#) o percentuale (%).

- **Disattivazione delle credenziali di autenticazione**

Le Società del Gruppo assicurano che le credenziali di autenticazione sono disattivate in caso di mancato utilizzo per un periodo temporale di almeno 3 mesi. La disattivazione delle credenziali avviene anche nel caso in cui il possessore non abbia più necessità di utilizzarle a causa del cambiamento delle proprie mansioni lavorative ovvero dell'interruzione del rapporto di lavoro.

- **Sospensione delle sessioni di lavoro**

Le Società del Gruppo obbligano gli utenti ad attivare il blocco del proprio computer quando si allontanano dalla propria postazione di lavoro anche per periodi di tempo limitati. Il blocco avviene comunque in maniera automatica dopo un lasso temporale di inattività prestabilito.

- **Firewalling e software antivirus**

Il sistema informativo delle Società del Gruppo è protetto contro gli accessi abusivi provenienti da reti pubbliche di comunicazioni.

Tutti gli elaboratori sono dotati di software antivirus aggiornati allo scopo di limitare il rischio di intrusione di virus e di programmi dannosi.

- **Aggiornamento dei programmi per elaboratore**

Le Società del Gruppo provvedono periodicamente all'installazione degli aggiornamenti (patch) per risolvere le problematiche emerse nel rispetto delle indicazioni e delle politiche in uso.

- **Backup e ripristino dei dati**

Le Società del Gruppo attuano azioni in grado di garantire la disponibilità delle informazioni in linea con le prescrizioni di legge, nonché verifiche periodiche dell'effettiva leggibilità e integrità delle informazioni salvate.

- **Strumenti elettronici per la protezione da accessi abusivi**

La rete informatica utilizzata dalle Società del Gruppo è protetta da specifici strumenti quali firewall, sistemi di Intrusion prevention e detection, in grado di ridurre il rischio di accessi abusivi.

- **Supporti removibili**

Le Società del Gruppo adottano specifici protocolli per la custodia, cancellazione e distruzione sicura sia dei supporti removibili utilizzati per il salvataggio o il trasferimento di dati personali sia degli elaboratori, fissi e portatili, in dismessi o non più utilizzati.

- **Controllo e custodia degli atti e dei documenti**

Le Società del Gruppo impartiscono indicazioni, in coordinamento con i Data Manager dei singoli Dipartimenti, affinché gli atti e i documenti cartacei siano controllati e custoditi dagli utenti durante tutte le operazioni di trattamento.

Tutto il personale delle Società del Gruppo è, in ogni caso, sempre responsabile dell'utilizzo e della custodia degli atti e dei documenti. Al termine delle operazioni di trattamento, gli atti e i documenti cartacei devono essere archiviati in armadi/cassetti muniti di serratura. Ove possibile, analoghe misure vanno adottate nel caso in cui l'utente si allontani temporaneamente dalla propria postazione.

- **Controllo e custodia degli atti e dei documenti contenenti dati particolari (i.e. sensibili o giudiziari)**

Le Società del Gruppo impartiscono indicazioni, in coordinamento con i Data Manager dei singoli Dipartimenti, affinché gli atti e i documenti cartacei contenenti dati sensibili e giudiziari siano utilizzati esclusivamente da personale espressamente incaricato al loro trattamento. Tali incaricati sono responsabili dell'utilizzo e della custodia degli atti e dei documenti che contengono tali categorie di dati particolari, in particolare, devono garantire che altri Incaricati non autorizzati non abbiano accesso ad informazioni che esulino dal proprio ambito di trattamento. Al termine delle operazioni di trattamento, gli atti e i documenti cartacei devono essere archiviati in armadi muniti di serratura.

- **Controllo degli accessi agli archivi contenenti dati particolari (i.e. sensibili o giudiziari)**

Solamente gli incaricati a ciò autorizzati hanno la possibilità di accedere agli archivi per lo svolgimento delle proprie mansioni lavorative. Al termine della giornata lavorativa e dopo l'orario di chiusura degli uffici, l'accesso agli archivi deve avvenire previa identificazione, anche mediante strumenti elettronici (ad es. badge).

- **Controllo degli accessi alle sedi delle Società del Gruppo**

L'accesso alle sedi delle Società del Gruppo è consentito al solo personale dipendente/collaboratori o a personale esterno autorizzato.

L'accesso alle sedi, da parte dei dipendenti è possibile solo mediante strumenti elettronici (ad es. badge) di identificazione, ovvero attraverso identificazione da parte degli addetti alla sorveglianza, o del personale preposto alla reception.

- **Controllo degli accessi ai Data Center**

Solamente gli utenti autorizzati dal Dipartimento EDP, o dal Management delle Società del Gruppo, possono accedere ai Data Center ove risiedono gli strumenti elettronici di trattamento.

- **Sistemi di videosorveglianza**

I sistemi di videosorveglianza, volti a rafforzare la sicurezza fisica delle sedi delle Società del Gruppo, sono implementati in coerenza con i provvedimenti del Garante e in coordinamento con il Dipartimento Segreteria Generale per quanto riguarda gli aspetti di tutela dei lavoratori (cfr. art. 4 Legge 300 del 1970).

H. Conservazione dei dati

Le Società del Gruppo adottano le misure per conservare le informazioni personali solo per il tempo necessario a soddisfare gli scopi per cui sono stati raccolti e comunque in maniera non eccedente rispetto a quanto richiesto da obblighi di legge.

I tempi di conservazione saranno regolati da idonee procedure operative e comunicati agli Interessati da apposite informative e secondo le indicazioni contenute in Provvedimenti del Garante ovvero indicate dalla normativa in vigore.

I. Controllo e conformità

Le Società del Gruppo stabiliscono procedure per controllare il rispetto dei principi previsti dal Regolamento.

E' responsabilità di tutto il personale delle Società del Gruppo conoscere, comprendere e rispettare questa Politica e i suoi contenuti.

La mancata osservanza potrebbe comportare rischi significativi per le Società del Gruppo, e può subordinare ciascun individuo ad azioni disciplinari, fino al licenziamento o all'interruzione del rapporto professionale.

In questo senso le Società del Gruppo pongono in essere periodici interventi di verifica del proprio sistema informativo per il tramite del personale coinvolto in base al livello di controllo posto in essere.

Le Società del Gruppo assicurano inoltre la raccolta delle eventuali segnalazioni di non conformità emerse sia in sede di analisi e/o sviluppo di nuovi prodotti, sia in fase di gestione ordinaria, indirizzandole verso i Data Manager dei diversi Dipartimenti e monitorando l'effettiva risoluzione.

J. Dati di contatto

Domande o dubbi sull'interpretazione o sulle modalità di applicazione della presente Policy possono essere rivolti scrivendo al Data Protection Officer, **Dott. Principe Nicola**, al seguente indirizzo email **DPO@grimaldi.napoli.it**.

3. I DIRITTI DELL'INTERESSATO

Il Regolamento riconosce al soggetto a cui si riferiscono i dati trattati (ad esempio il cliente, il socio, il dipendente, ecc.) taluni di diritti volti a garantire un adeguato e diretto controllo sul rispetto da parte delle Società del Gruppo dei limiti e delle condizioni poste al Trattamento dei dati personali.

Le Società del Gruppo si impegnano a garantire l'efficace esecuzione dei processi necessari all'esercizio dei diritti degli Interessati (es. Clienti, fornitori, personale, etc.).

Nei paragrafi successivi si riportano le linee guida e la tipologia di richieste che ogni interessato ha il diritto di esercitare con particolare riferimento a:

- Diritto di accesso ai dati da parte dell'Interessato
- Diritto di rettifica
- Diritto di cancellazione
- Diritto di limitazione di Trattamento
- Diritto alla portabilità dei dati
- Diritto di opposizione

3.1 Esercizio dei diritti dell'Interessato e Tempi di Riscontro

L'Interessato ha la facoltà di esercitare i propri diritti secondo le modalità e nei limiti previsti dal Regolamento. Le Società del Gruppo si impegnano a fornire all'Interessato le informazioni relative all'azione intrapresa riguardo a una richiesta senza ingiustificato ritardo e, comunque, al più tardi **entro 30 giorni** dal ricevimento della richiesta stessa. Tale termine potrà essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. Inoltre, le Società del Gruppo si impegneranno a informare l'Interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta. Se la richiesta dell'Interessato sarà presentata mediante mezzi elettronici, le informazioni saranno fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'Interessato.

Tali diritti potranno essere esercitati attraverso l'invio di una mail all'indirizzo ***privacy@grimaldi.napoli.it*** oppure tramite comunicazione scritta, specificando l'oggetto della richiesta, all'attenzione del ***Responsabile Protezione Dati*** (di seguito "DPO"), ***Dott. Nicola Principe***, domiciliato per la carica presso la sede della Società sita in Via Marchese Campodisola, 13, 80133 Napoli NA.

Una volta ricevuta la richiesta, la Segreteria Generale, ovvero il DPO qualora la richiesta sia allo stesso indirizzata, non possono rifiutarsi di soddisfare la richiesta dell'interessato, salvo che le Società del Gruppo dimostrino che non siano in grado di identificare l'interessato. Qualora l'interessato sia identificabile, Segreteria Generale ovvero il DPO devono inviare tramite mail o, se ricevuta in forma cartacea consegnare a vista, la stessa ai Data Manager di riferimento entro due giorni dalla ricezione della stessa.

In particolare, in base ai contenuti della richiesta e alla tipologia di Interessato che la effettua, vengono indirizzate a:

- Passenger Department per le richieste provenienti in ambito passeggeri;
- Corporate Short Sea Shipping Commercial Department per le richieste provenienti in ambito Cargo;

- Purchasing Department per le richieste provenienti da Terze Parti/Fornitori;
- Human Resources Department per le richieste provenienti da dipendenti di Sede e Candidati;
- Crew Department per le richieste provenienti da dipendenti Marittimi e Candidati.

I singoli Data Manager provvederanno a notificare la presa in carico della richiesta attraverso comunicazione tramite mail o attraverso comunicazione scritta a Segreteria Generale o al DPO entro un giorno dalla ricezione della stessa. Il Data Manager con il supporto del DPO dovrà valutare se le richieste saranno manifestamente infondate e/o richiedano un effort economico non proporzionale alla richiesta, in particolare per il loro carattere ripetitivo. In tal caso le Società del Gruppo potranno valutare la possibilità di:

- addebitare i costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta all'Interessato;
- rifiutare di evadere la richiesta informando e motivando tale decisione all'Interessato.

Il Data Manager provvederà entro 7 giorni a notificare alle Società del Gruppo la valutazione in merito alla fondatezza/infondatezza della richiesta. Qualora la richiesta sia ritenuta infondata e quindi non si ottempera alla richiesta dell'interessato, le Società del Gruppo informano l'interessato senza ritardo, e al più tardi entro un mese dal ricevimento della richiesta, dei motivi dell'inottemperanza, della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale. Qualora la richiesta sia ritenuta fondata, per l'evasione i singoli Data Manager, con il supporto degli Autorizzati al Trattamento, provvederanno a prendere in carico le stesse rispetto al proprio ambito di competenza e alla procedura operativa adottata da ogni singolo dipartimento. Tali procedure prevedono la piena responsabilità di ogni singolo Data Manager durante tutte le fasi di gestione delle richieste, sia nel caso in cui il dato sia archiviato in formato cartaceo sia nel caso in cui le attività necessarie all'esercizio dei diritti dei singoli interessati prevedano azioni tecniche sui sistemi informatici della Società. In questo ultimo caso, i singoli Data Manager saranno eventualmente supportati da Software Projects Design and Management Department per le richieste provenienti dagli interessati in ambito Cargo e dal dipartimento EDP per tutte le altre tipologie. Qualora il Data Manager abbia la necessità di un supporto in ambito normativo e/o legale potrà consultare il DPO.

Le Società del gruppo si impegnano a mettere a disposizione di ogni singolo Data Manager un registro delle richieste con il duplice scopo di tracciare la gestione di talune richieste, rispettando il principio di accountability, e di armonizzare il processo fra tutti i dipartimenti al fine di evitare potenziali errori/duplicazioni di richieste pervenute al Titolare.

Entro 7 giorni dall'esito della valutazione della richiesta dovranno essere terminate le attività utili all'evasione della stessa. In particolare il Data Manager invierà comunicazione alle Società del Gruppo con allegata la documentazione prodotta o evidenze delle azioni svolte per evadere la richiesta. Queste ultime, supportate dal DPO o da Segreteria Generale, comunicheranno entro 7 giorni gli esiti all'interessato.

3.2 Diritto di accesso ai dati da parte dell'Interessato

L'Interessato ha il diritto di ottenere dalle Società del Gruppo la conferma che sia o meno in corso un Trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

- le finalità del Trattamento;
- le categorie di dati personali in questione;

- i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
- quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- l'esistenza del diritto dell'Interessato di chiedere alle Società del Gruppo 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 di proporre reclamo a un'autorità di controllo;
- qualora i dati non siano raccolti presso l'Interessato, tutte le informazioni disponibili sulla loro origine.

Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'Interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate.

Le Società del Gruppo forniscono una copia dei dati personali oggetto di Trattamento. In caso di ulteriori copie richieste dall'Interessato, le Società del Gruppo possono addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'Interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'Interessato, le informazioni sono fornite in un formato elettronico di uso comune

3.3 Diritto di rettifica

L'Interessato ha il diritto di ottenere dalle Società del Gruppo la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del Trattamento, l'Interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

3.4 Diritto di cancellazione

L'Interessato ha il diritto di ottenere dalle Società del Gruppo la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e le Società del Gruppo hanno l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:

- i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
- l'Interessato revoca il consenso su cui si basa il Trattamento e se non sussiste altro fondamento giuridico per il Trattamento;
- l'Interessato si oppone al Trattamento e non sussiste alcun motivo legittimo prevalente per procedere al Trattamento;
- i dati personali sono stati trattati illecitamente;
- i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui sono soggette le Società del Gruppo;
- i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione

Quanto sopra riportato non si applica nella misura in cui il Trattamento sia necessario:

- per l'esercizio del diritto alla libertà di espressione e di informazione;
- per l'adempimento di un obbligo legale che richieda il Trattamento previsto dal diritto dell'Unione o dello Stato membro cui sono soggette le Società del Gruppo o per l'esecuzione di un compito

svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui sono investite le Società del Gruppo;

- a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici nella misura in cui si rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale Trattamento;
- per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

3.5 Diritto di limitazione di Trattamento

L'Interessato ha il diritto di ottenere dalle Società del Gruppo la limitazione del Trattamento quando ricorre una delle seguenti ipotesi:

- l'Interessato contesta l'esattezza dei dati personali, per il periodo necessario alle Società del Gruppo per verificare l'esattezza di tali dati personali;
- il Trattamento è illecito e l'Interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
- benché le Società del Gruppo non ne abbiano più bisogno ai fini del Trattamento, i dati personali sono necessari all'Interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
- l'Interessato si è opposto al Trattamento in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi delle Società del Gruppo rispetto a quelli dell'Interessato.

Se il Trattamento è limitato tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'Interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.

L'Interessato che ha ottenuto la limitazione del Trattamento è informato dalle Società del Gruppo prima che detta limitazione sia revocata.

3.6 Diritto alla portabilità dei dati

L'Interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti alle Società del Gruppo e ha il diritto di trasmettere tali dati a un altro Titolare del Trattamento senza impedimenti da parte del Titolare del Trattamento cui li ha forniti qualora:

- a) il Trattamento si basi sul consenso su un contratto;
- b) il Trattamento sia effettuato con mezzi automatizzati.

Nell'esercitare i propri diritti relativamente alla portabilità dei dati l'Interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un Titolare del Trattamento all'altro, se tecnicamente fattibile.

Tale diritto non si applica al Trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui sono investite le Società del Gruppo.

3.7 Diritto di opposizione

L'Interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al Trattamento dei dati personali che lo riguardano compresa la profilazione sulla base di tali disposizioni. Le Società del Gruppo si astengono dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al Trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'Interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria. Qualora i dati personali siano trattati per finalità di marketing diretto, l'Interessato ha il diritto di opporsi in qualsiasi momento al Trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto. Qualora l'Interessato si opponga al Trattamento per finalità di marketing diretto, i dati personali non sono più oggetto di Trattamento per tali finalità.

Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici l'Interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al Trattamento di dati personali che lo riguarda, salvo se il Trattamento è necessario per l'esecuzione di un compito di interesse pubblico.