GRUPPO d'Amico

d'Amico Società di Navigazione S.p.A.

REGOLAMENTO PRIVACY DI GRUPPO

(contenente le "Norme Vincolanti di Impresa" ex REGOLAMENTO UE 679/2016)

INDICE

PREMESSA

La società D'Amico Società di Navigazione S.p.A. (di seguito per brevità DSN) e le società in scope (così come declinate nell'Allegato 1 al presente documento) effettuano il trattamento dei dati personali delle seguenti categorie di interessati individuate:

- Personale di Terra subordinato e parasubordinato e personale di bordo1;
- Candidati;
- Clienti e Prospect;
- Fornitori2;
- Visitatori;
- Componenti degli Organi e Organismi interni di D'Amico (OdV, Collegio Sindacale e CdA);

nel rispetto dei principi di liceità, correttezza, trasparenza ed esattezza stabiliti dal Regolamento n. 679/2016.

Per garantire che il trattamento dei dati personali delle categorie di interessati sopra riportate venga effettuato nel rispetto dei principi sanciti dalla normativa vigente, DSN e le società in scope al modello hanno implementato un sistema per la gestione della privacy che è illustrato nell'Allegato 1 alle presenti norme.

A completamento del modello privacy di gruppo DSN ha formalizzato le presenti norme vincolanti d'impresa, che rappresentano uno degli strumenti di compliance al Regolamento UE n. 679/2016, di

[1] In tale categoria di interessati rientrano tutti i dipendenti a tempo determinato o indeterminato e i Marittimi.

[2] In tale categoria di interessati rientrano anche i Professionisti Esterni.

seguito per brevità il Regolamento, con specifico riferimento alla fattispecie di "*trasferimento di dati al di fuori dell'UE*" per quanto riguarda le seguenti categorie di interessati

- Personale di Terra subordinato e parasubordinato e personale di bordo
- Candidati
- Membri degli organi e organismi interni

1. INTRODUZIONE

Le presenti Norme Vincolanti d'Impresa (BCR – Binding Corporate Rules) rappresentano lo strumento unilaterale attraverso cui d'Amico Società di Navigazione S.p.A., di seguito DSN, in qualità Holding del gruppo d'Amico, intende fornire le *garanzie adeguate* richieste per il trasferimento di dati all'interno del Gruppo verso Paesi terzi extra UE alle categorie di interessati individuate (dipendenti e collaboratori, candidati, membri degli organi e organismi interni), in assenza delle decisioni adeguate di cui al CAPO V "*Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali*".

Dette norme stabiliscono le regole per la corretta applicazione delle politiche in materia di protezione dei dati personali e sono giuridicamente vincolanti per tutte le società del gruppo, compresi i dipendenti del gruppo. Le presenti norme assicurano il rispetto dei requisiti in materia di protezione dei dati e dei diritti degli interessati, a cui sono espressamente conferiti diritti azionabili in relazione al trattamento dei dati personali ad essi riferiti.

Si specifica che DSN ha definito la forma, il contenuto e il campo delle norme vincolanti d'impresa in conformità con quanto stabilito dal Capo V, Articolo 47 Regolamento UE 2016/679, recante "Norme vincolanti d'impresa".

1.1. Principali definizioni

Il Regolamento propone il "*vocabolario essenziale*" in tema di protezione dei dati personali. Si riportano di seguito le principali definizioni.

dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); 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.

trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, 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.

limitazione di trattamento: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro.

impresa: si intende la persona fisica o giuridica che esercita un'attività economica, (ivi comprese le società di persone o le associazioni che esercitano regolarmente un'attività economica).

gruppo imprenditoriale: si definisce un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate.

autorità di controllo: si intende l'autorità pubblica indipendente istituita da uno Stato membro per il controllo del rispetto della normativa in materia di protezione dei dati personali.

1.2. Struttura del Documento

Il presente documento, conformemente a quanto previsto dal Regolamento, è strutturato nelle seguenti sezioni:

1. La struttura e le coordinate di contatto di DSN e sue controllate.
2. Le categorie di dati personali, le tipologia di trattamento e relative finalità, le categorie di interessati a cui si riferiscono i dati e paesi terzi verso cui vengono trasferiti i dati in questione.
3. La natura giuridicamente vincolante delle presenti norme sia a livello interno che esterno al gruppo.
4. L'esplicitazione dei principi generali di protezione dei dati, con particolare riferimento alla limitazione del loro utilizzo esclusivamente per le finalità per le quali vengono acquisiti, alla limitazione del periodo di conservazione, alla qualità dei dati, al rispetto dei principi di *privacy by design* e *privacy*

by default, alla base giuridica del trattamento, alle misure a garanzia della sicurezza dei dati e ai requisiti per i successivi, eventuali trasferimenti ad Organismi che non sono vincolati dalle presenti norme vincolanti.

5. I diritti degli interessati in relazione al trattamento e relativi mezzi per esercitarli, ivi compresi il diritto di non essere sottoposti a profilazione, di proporre reclamo all'Autorità di Controllo competente e di ricorrere alle Autorità giurisdizionali competenti degli Stati membri UE, nonché il diritto di ottenere la riparazione e, se del caso, il risarcimento per violazione delle norme vincolanti d'impresa (c.d. "clausola del terzo beneficiario").
6. L'assunzione di responsabilità da parte di DSN e sue controllate per qualunque violazione delle norme vincolanti d'impresa commesse da una società appartenente al gruppo e non stabilita nell'Unione.
7. Le modalità in base alle quali sono fornite agli interessati le informazioni sulle norme vincolanti d'impresa.
8. I compiti del Data Protection Officer (DPO) designato al controllo del rispetto delle norme vincolanti d'impresa e il controllo della formazione e della gestione dei reclami.
9. Le procedure di reclamo.
10. I meccanismi all'interno del gruppo per garantire la verifica della conformità alle norme vincolanti d'impresa. Tali meccanismi comprendono verifiche sulla protezione dei dati e metodi per assicurare provvedimenti correttivi intesi a proteggere i diritti dell'interessato. I risultati di tali verifiche sono comunicati al DPO, al CdA di DSN e sono resi disponibili su richiesta all'Autorità di Controllo competente.
11. I meccanismi per riferire e registrare le modifiche delle norme e comunicarle all'Autorità di Controllo.
12. Il meccanismo di cooperazione con l'Autorità di Controllo per garantire la conformità da parte di ogni società del gruppo, in particolare la messa a disposizione dell'Autorità di Controllo dei risultati emersi dall'attività di controllo interna.

13. I meccanismi per segnalare all'Autorità di Controllo competente ogni requisito di legge cui potrebbe essere soggetta una società del gruppo in un paese terzo, che potrebbe avere effetti negativi sostanziali sulle garanzie fornite dalle norme vincolanti d'impresa.
14. La formazione in materia di protezione dei dati al personale che ha accesso permanente o regolare ai dati personali.

1.3. Scopo e campo di applicazione

Il campo di applicazione delle presenti Norme Vincolanti d'Impresa è il trattamento dei dati personali riferiti alle seguenti categorie di interessati:

- Personale di terra e del personale di bordo
- Candidati
- Membri degli organi e organismi interni

effettuato tra le società del gruppo (infra-gruppo) e che possono essere oggetto di trasferimento al di fuori dell'Unione Europea per finalità di gestione amministrativo-contabile.

Si specifica che il trattamento viene effettuato sia in modalità cartacea sia in modalità informatica.

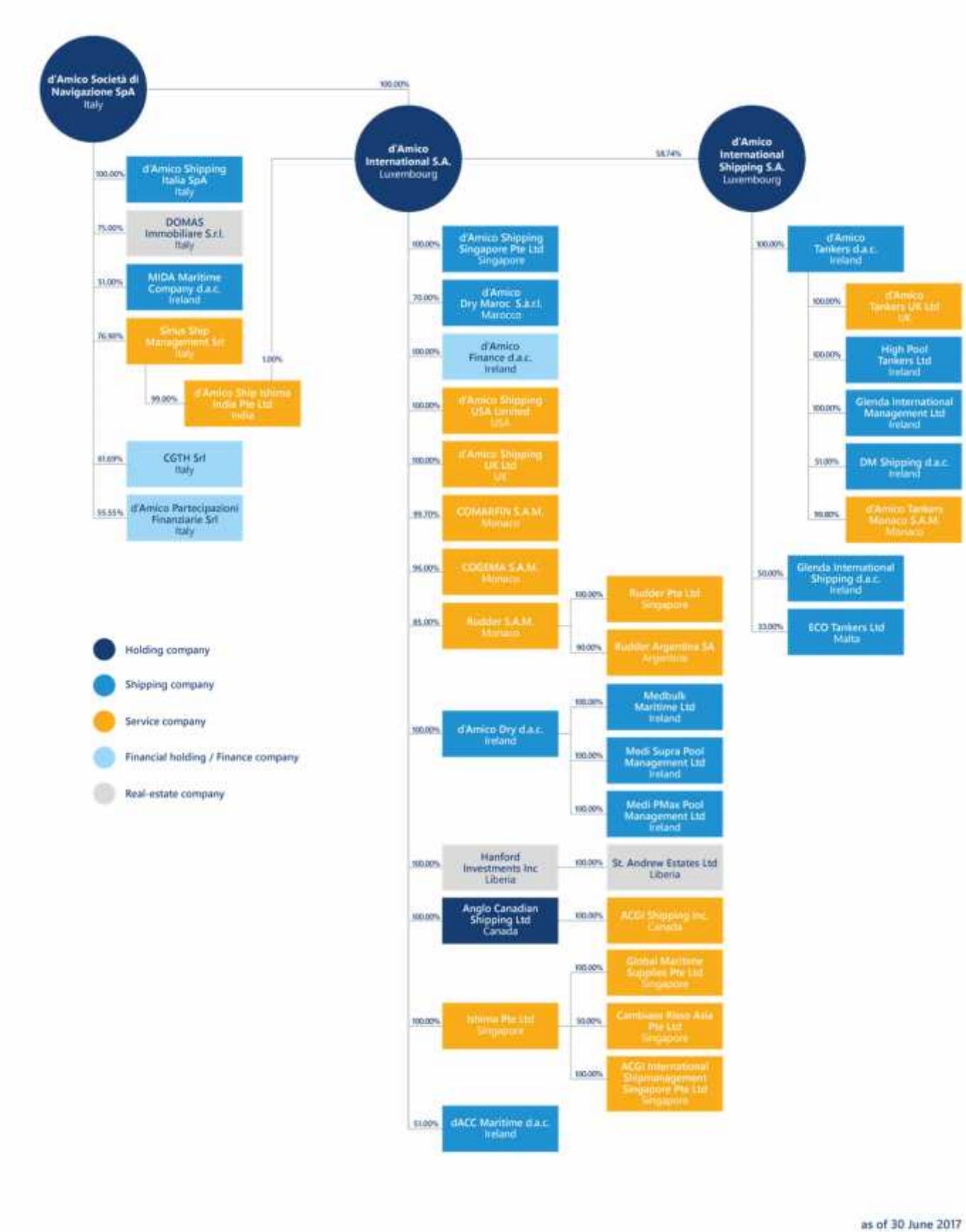
2. LA STRUTTURA E LE COORDINATE DI CONTATTO DEL GRUPPO

Il gruppo d'Amico è attualmente composto da 41 (quarantuno) società, operanti nei seguenti paesi:

- Italia
- Lussemburgo
- Principato di Monaco
- Regno Unito
- Irlanda
- Malta
- USA
- Canada
- Singapore
- India
- Marocco
- Argentina
- Liberia

secondo la struttura di partecipazioni sotto riportata.

References: Regolamento UE n. 679/2016



Il gruppo d'Amico, fondato nel 1952, è tra i leader mondiali nel trasporto marittimo nei settori dry cargo e product tankers, e nei servizi strumentali alle attività di core business. Dispone di una tra le più importanti flotte a livello mondiale di navi portarinfuse e navi cisterna. Con uffici in più di 10 sedi nel mondo, il gruppo d'Amico impiega 1.620 dipendenti, di cui 1.294 in qualità di Personale di bordo e 326 in qualità di Personale di terra.[3]

Da sempre il rispetto e la salvaguardia dell'ambiente, l'attenzione al cliente e l'eccellenza professionale del proprio personale rappresentano i capisaldi della propria mission e i principi della propria strategia.

L'Head Quarter del gruppo si trova a Roma.

Si riportano di seguito i dati di contatto

Rome – Head Office

Corso d'Italia 35/B, Rome, 00198, Italy

P +39 06 845 611

F +39 06 98968092

E info@damicoship.com

[3] Dato al 31.12.2016 (Fonte Annual Report)

3. LE CATEGORIE DI INTERESSATI/DATI PERSONALI/TRATTAMENTI/PAESI VERSO CUI I DATI VENGONO TRASFERITI

DSN, nell'ambito delle attività di assessment per la messa a punto del modello privacy di gruppo, ha identificato le seguenti categorie di Interessati per le quali si potrebbe configurare il trasferimento di dati verso paesi extra UE:

- Personale di terra subordinato e parasubordinato e personale di bordo
- Candidati
- Membri degli organi e organismi interni

Per dette categorie di Interessati sono riportate, nelle tabelle successive, le seguenti informazioni:

- Categoria di dati trattati: indica la tipologia di dati gestiti per ciascuna categoria di interessati.
- Finalità del trattamento: indica le motivazioni o le attività inerenti allo specifico trattamento dei dati.
- Base giuridica del trattamento: indica la base su cui si fonda il trattamento, con riferimento all'art. 6 "*Liceità del trattamento*" del Regolamento.
- Modalità di trattamento: indica il nome dell'applicativo (nel caso in cui l'archiviazione è effettuata in modalità elettronica) o dell'archivio (nel caso in cui l'archiviazione è effettuata in modalità cartacea) utilizzato per la gestione dei dati relativi a ciascuna classe di interessati.
- Paese verso cui i dati possono essere trasferiti: identifica, ove applicabile, il paese terzo e/o dell'organizzazione internazionale verso il quale si effettua un trasferimento di dati personali.

Personale di Terra subordinato e parasubordinato e Personale di bordo

Categoria di dati	Finalità del trattamento	Base giuridica del trattamento	Modalità	
			Elettronico	Cartaceo
Dati personali comuni (dati anagrafici, istruzione e cultura ecc.) Dati inerenti la Salute/, malattie professionali Dati Amministrativo-Contabili Paghe/ritenute sindacali Dati di carattere professionale	*Finalità amministrativo-contabili*: ▪ Gestione del personale (reclutamento, selezione, valutazione e monitoraggio del personale, test attitudinali, formazione). ▪ Trattamento giuridico ed economico del personale (calcolo e pagamento di retribuzioni ed emolumenti vari; applicazione della legislazione previdenziale ed assistenziale; cassa integrazione e guadagni). ▪ Adempimento di obblighi fiscali o contabili. ▪ Adempimenti connessi al versamento delle quote di iscrizione ai sindacati o all'esercizio di diritti sindacali (gestione di permessi, distacchi, ecc.) Igiene e sicurezza del lavoro. ▪ Organizzazione, gestione amministrativa e controllo delle trasferte aziendali. ▪ Gestione del contenzioso. *Finalità connesse al settore bancario, creditizio e assicurativo*: ▪ Servizi assicurativi (responsabilità civile, ramo vita, sanità e calamità).	- L'interessato ha espresso il consenso al trattamento dei propri dati personali per le specifiche finalità (rif. art. 6, lettera a. del Regolamento). - Il trattamento è necessario all'esecuzione di un contratto (rif. art. 6, lettera b. del Regolamento)	- Nordic IT - IT2 - Sharepoint - Zantaz - Tagetik - DUALOG - OMNIA (Database personale di bordo gestito da Sirius Ship Management - Exchange Server - HRM (software per la gestione delle risorse umane per il gruppo - Staff Attendance - Travel and expenses - D'Amico Welfare - Whistleblowing - Watckeeper	- Archivio cartaceo presso l'HR Dept. della capogruppo ed archivi locali nelle sedi internazionali del gruppo.

Organizzazioni verso cui i dati sono trasferiti:	Estremi identificativi dei destinatari dei dati personali
Società del gruppo	d'Amico Società di Navigazione S.p.A. e società controllate e/o collegate collocate nei seguenti paesi extra UE: Principato di Monaco, Singapore, India, Marocco, USA e Liberia
Società Esterne	Ernst Young per payroll service, ADP per USA.

Candidati e colloquiandi

Categoria di dati	Finalità del trattamento	Repository	
		Elettronico	Cartaceo
Dati personali comuni (dati anagrafici, istruzione e cultura ecc.) Dati personali sensibili (se presenti nel CV)	*Finalità amministrativo-contabili*: ▪ acquisizione di dati nella fase di screening della candidatura ▪ valutazione del curriculum. ▪ effettuazione dei colloqui. ▪ gestione degli adempimenti pre-assunzione	- Database raccolta cv sito Internet Sharepoint[4] - Exchange Server - Nordic IT - IT2 - Zantaz - Tagetik - DUALOG	- Archivio cartaceo presso l'HR Dept. di DSN.

Categorie di destinatari che concorrono al trattamento:	Estremi identificativi del Destinatario *(ex. Ragione Sociale; Nome e Cognome; Nome del dipartimento)*
Società del Gruppo	d'Amico Società di Navigazione S.p.A. e società controllate anche extra UE
Società Esterne	n.a.

[4] Si specifica che il database è gestito da HR Group e HR Local Manager o ruolo più generalista. Esistono due profili: admin su ROMA HR e Comunicazione e recruiter Dublino e Singapore.

Componenti degli Organi e Organismi interni i D'Amico (CdA, Collegio Sindacale, OdV e Comitati interni)

Categoria di dati	Finalità del trattamento	Repository	
		Elettronico	Cartaceo
Dati personali comuni (dati anagrafici, istruzione e cultura, ecc)	*Finalità amministrativo-contabili:* ✓ valutazione dell'idoneità del profilo rispetto alla carica ricoperta. ✓ formalizzazione e gestione degli incarichi e dei relativi pagamenti legati a compensi/rimborsi spese. ✓ adempimento di obblighi amministrativi, assicurativi, fiscali. ✓ gestione del contenzioso e precontenzioso.	- Multipartner - Nordic IT - IT2 - Zantaz - Tagetik - DUALOG - Exchange Server	- Archivio cartaceo presso il Legal & Insurance Dept. di DSN.
Dati Amministrativo-Contabili			

Categorie di destinatari che concorrono al trattamento:	Estremi identificativi del Destinatario *(ex. Ragione Sociale; Nome e Cognome; Nome del dipartimento)*
Società del Gruppo	d'Amico Società di Navigazione S.p.A. e società controllate anche extra UE
Società Esterne	Società di selezione del personale in qualità di Responsabili esterni del trattamento dei dati

4. LA NATURA GIURIDICAMENTE VINCOLANTE DELLE PRESENTI NORME A LIVELLO SIA INTERNO CHE ESTERNO DEL GRUPPO

Le presenti norme sono sottoscritte per accettazione incondizionata da tutte le società appartenenti al gruppo d'Amico e sono, pertanto, giuridicamente vincolanti sia all'interno del gruppo sia all'esterno.

Sulla base di quanto contenuto nelle presenti norme, DSN effettua degli audit a campione su base annuale presso le sedi dei paesi extra EU.

Tali audit sono pianificati e gestiti dal Data Protection Officer di gruppo sulla base di un piano di audit annuale, con il supporto dei Coordinatori Privacy.

Alla società sarà fornito un lasso di tempo sufficiente a sopperire alle eventuali carenze rilevate all'interno del sistema di gestione dei dati personali di cui alle presenti norme.

Le presenti norme sono vincolanti anche per tutti i soggetti che gestiscono dati degli interessati sopra descritti in qualità di Responsabili esterni del trattamento dei dati per le società del gruppo al di fuori dell'Unione Europea (fornitori e professionisti), per i quali è prevista l'accettazione delle stesse nell'ambito dei contratti commerciali.

5. I PRINCIPI GENERALI DI PROTEZIONE DEI DATI

DSN e le società "in scope" al modello hanno messo in atto le misure tecniche e organizzative per garantire un livello di sicurezza proporzionato al rischio, che comprendono, tra le altre:

- la pseudonimizzazione e la cifratura dei dati personali.
- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento.
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico.
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Il tutto rispettando i principi di *privacy by design* e *privacy by default* centrali nel modello organizzativo privacy del gruppo d'Amico.

In particolare DSN, in qualità di Holding del gruppo d'Amico, ha realizzato le attività di analisi e valutazione dei rischi, così come previsto dal Regolamento, di cui si riporta un estratto in Allegato 2 al presente documento

6. I DIRITTI DEGLI INTERESSATI E LA PROTEZIONE DEI DATI PERSONALI

DSN e società in scope al modello hanno impostato un sistema organizzativo privacy in grado di assicurare il rispetto dei diritti degli interessati, come previsti al CAPO III del Regolamento recante "*Diritti dell'interessato*".

In particolare, per quanto riguarda la categorie di interessati relative a:

- Personale di terra subordinato e parasubordinato e Personale di bordo
- Candidati
- Membri degli organi e organismi interni

DSN e società in scope forniscono l'informativa ai sensi dell'art. 13 del Regolamento, informando gli interessati del possibile trasferimento dei dati personali che li riguardano a società del gruppo controllate anche al di fuori dell'Unione Europea ed acquisendo il relativo consenso.

L'informativa contiene tutte le informazioni previste dal Regolamento, ivi compresi i diritti degli interessati e le relative modalità di esercizio.

In particolare:

- diritto di accesso;
- diritto di rettifica e cancellazione;
- diritto di limitazione al trattamento;
- diritto di opposizione.

I diritti possono essere esercitati inviando una richiesta indirizzata al DPO di gruppo per e-mail.

6.1. Clausola del terzo beneficiario

Si specifica che, ai sensi delle presenti Norme Vincolanti d'Impresa, i soggetti interessati hanno il diritto di far valere le BCR contro qualsiasi società del Gruppo d'Amico che abbia violato le presenti Norme presentando un reclamo alle Autorità di Controllo competenti, ivi compreso il diritto dei soggetti interessati ad ottenere il risarcimento del danno connesso al mancato rispetto di quanto previsto dalle presenti norme

non solo nei confronti del Titolare del trattamento dei dati, bensì anche nei confronti dei Responsabili esterni del trattamento o degli eventuali sub Responsabili esterni del trattamento, qualora il diretto destinatario della richiesta risarcitoria risulti scomparso o abbia giuridicamente cessato di esistere.

7. LA RESPONSABILITÀ DI DSN E SOCIETÀ IN SCOPE AL MODELLO IN QUALITÀ DI AUTONOMI TITOLARI DEL TRATTAMENTO

DSN e società in scope ottemperano alle previsioni del Regolamento per quanto riguarda le responsabilità del Titolare, coerentemente con il CAPO IV recante "*Titolare del trattamento e responsabile del trattamento*".

In particolare DSN in qualità di Holding del gruppo d'Amico, ha messo in atto un sistema di tutela e garanzia della riservatezza e dei diritti degli interessati, che viene aggiornato costantemente, e che garantisce misure tecniche ed organizzative adeguate ai trattamenti effettuati.

L'obiettivo del sistema è quello di garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari al perseguimento delle specifiche finalità del trattamento, sia per quanto riguarda la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità.

Il sistema garantisce, infine, che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

A questo fine DSN, in qualità di Holding del gruppo d'Amico, ha definito la propria organizzazione privacy, articolata come segue:

7.1. TITOLARE (ART.24)

In qualità di autonomi Titolari del trattamento, DSN in qualità di Holding del gruppo d'Amico e e società in scope al modello, sono i destinatari principali di tutte le obbligazioni previste dal Regolamento; in quanto tali hanno le seguenti responsabilità:

- implementare misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento. Dette misure sono riesaminate e aggiornate qualora necessario;
- aderire ai codici di condotta (cfr. art. 40) o a meccanismi di certificazione (cfr. art. 42) al fine di dimostrare il rispetto degli obblighi previsti dal Regolamento;
- designare per iscritto, ove applicabile, un rappresentante nell'Unione (cfr. art. 27);

- individuare e nominare i Responsabili dei trattamenti (cfr. art. 28 e art. 29);
- cooperare, su richiesta, con l'Autorità di Controllo nell'esecuzione dei suoi compiti (cfr. art. 31);
- notificare, in caso di violazione dei dati personali, all'Autorità di Controllo competente la violazione a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'Autorità di Controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo (cfr. art .33);
- dimostrare che l'Interessato ha prestato il consenso al trattamento dei propri dati personali (cfr. art 7);
- assicurarsi che il Responsabile della Protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali (cf. art. 38);
- sostenere il Responsabile della Protezione dei dati nell'esecuzione dei compiti (cfr. art. 39), fornendo le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica (cf. art. 38);
- assicurarsi che il Responsabile della Protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti (cf. art. 38).

7.2. RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO) (ART. 37)

In ottemperanza all' art. 37 del Regolamento, DSN in qualità di Holding del gruppo d'Amico, ha designato un unico Responsabile della Protezione dei dati, di seguito DPO in staff al Titolare del Trattamento di DSN, la Dott.ssa Marzia Vona.

La nomina del DPO è stata formalizzata attraverso una lettera di nomina che ne disciplina in modo dettagliato i compiti; copia di tale lettera di nomina controfirmata dal DPO è archiviata presso l'ufficio HR.

Il DPO, conformemente a quanto previsto dall'articolo 38 del Regolamento:

- deve essere tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali; devono essergli fornite le risorse necessarie per assolvere tali compiti e, quindi, anche un budget di spesa;
- non è penalizzato dal Titolare del trattamento o dal Responsabile del trattamento per l'adempimento dei propri compiti;
- riferisce direttamente al vertice gerarchico del Titolare del trattamento o del Responsabile del trattamento;
- può essere contattato dagli Interessati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal Regolamento;
- è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri;
- può svolgere altri compiti e funzioni purché non diano adito a un conflitto di interessi.

La *governance* del sistema di gestione privacy attraverso tale figura consentirà al gruppo d'Amico non solo il rispetto delle prescrizioni in tema di *data protection*, ma anche il controllo dei profili di responsabilità giuridica derivanti dall'applicazione del *principio dell'accountability*.

Di seguito vengono elencati i principali compiti in capo al DPO:

a) coordinare e gestire i Coordinatori privacy nominati dal Titolare del trattamento per ogni sede del gruppo;
b) informare e fornire consulenza al Titolare del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento, nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
c) sorvegliare sull'osservanza del Regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati, nonché delle politiche del Titolare 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;
d) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;
e) cooperare con l'autorità di controllo;

f) 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.

7.3. COORDINATORE PRIVACY (ART.37)

DSN, in qualità di Holding del gruppo d'Amico, al fine di agevolare il coordinamento e la gestione delle azioni volte al rispetto del Regolamento, ha nominato, per ogni country del gruppo a livello internazionale delle società in scope al modello, un Coordinatore Privacy.

Tale figura è coordinata dal DPO di Gruppo.

La nomina dei singoli Coordinatori Privacy è formalizzata attraverso una lettera di nomina che ne disciplina in modo dettagliato i compiti; copia delle lettere di nomina controfirmate dai Coordinatori Privacy sono archiviate presso HR Department.

7.4. RESPONSABILE DEL TRATTAMENTO (ART. 28 E ART. 29)

Ai sensi dell'articolo 28 del Regolamento, "*qualora un trattamento debba essere effettuato per conto del Titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti richiesti dal Regolamento Europeo e garantisca la tutela dei diritti dell'interessato*".

Il Responsabile del trattamento dei dati personali (di seguito Responsabile) è pertanto individuato dal Titolare tra soggetti che per esperienza, capacità ed affidabilità, siano in grado di fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza dei dati personali gestiti (sia con l'ausilio di strumenti informatici che non).

All'interno del gruppo d'Amico la figura del Responsabile è stata distinta tra:

- *Responsabile interno Privacy;*
- *Responsabile esterno Privacy*.

7.4.1. RESPONSABILI INTERNI PRIVACY

DSN e le società in scope al modello che presentano una complessità organizzativa maggiore in funzione del numero di dipendenti, in qualità di autonomi Titolari del Trattamento, hanno nominato in qualità di Responsabili interni del Trattamento dei dati, i Responsabili delle Funzioni Organizzative, che nell'ambito delle proprie attribuzioni, trattano manualmente o con strumenti elettronici, dati personali di cui DSN e le società in scope sono Titolari.

Le nomine sono formalizzate attraverso una lettera di nomina che ne disciplina in modo dettagliato i compiti; copia delle lettere di nomina controfirmate dai Responsabili interni Privacy sono archiviate presso l'HR Dept di DSN.

Modifiche organizzative che possono avere un impatto sull'organizzazione dei Responsabili interni Privacy devono essere comunicate al DPO, che valuta e propone ai Titolari del trattamento eventuali variazioni da apportare all'organizzazione.

7.4.2. RESPONSABILI ESTERNI PRIVACY

DSN e tutte le società in scope e out of scope al modello sono Responsabile Esterni del trattamento dei dati per le altre società del gruppo (ciascuna società è Responsabile esterno del trattamento per tutte le altre), a prescindere dai contratti commerciali infragruppo in essere. Tale scelta è motivata dal fatto che non è possibile escludere che, al di fuori degli accordi commerciali formalizzati, possa configurarsi comunque un eventuale transito di dati personali riferiti agli interessati.

Tutte le società e i professionisti che forniscono servizi alle singole società del gruppo in scope al modello, che nell'ambito dell'incarico ricevuto trattano manualmente o con strumenti elettronici, dati personali di cui DSN e le società in scope sono Titolari.

7.5. CLASSI DI INCARICATI

DSN e le società in scope al modello, in qualità di autonomi Titolari del Trattamento, hanno individuato differenti Classi di Incaricati nelle quali rientrano tutti i dipendenti e collaboratori delle varie società del Gruppo che, nell'ambito delle proprie mansioni, trattano manualmente o con strumenti elettronici, dati personali di cui DSN e le società in scope sono Titolari.

Tale designazione è formalizzata attraverso apposita lettera che ne disciplina i compiti; le copie delle lettere di designazione controfirmate per presa visione dagli incaricati sono archiviate dal DPO presso il proprio ufficio.

7.6. AMMINISTRATORI DI SISTEMA (ADS)

DSN e le società in scope al modello, in qualità di autonomi Titolari del Trattamento, hanno nominato in qualità di Amministratori di Sistema, i dipendenti e collaboratori con particolari compiti e responsabilità nell'ambito della gestione e manutenzione delle applicazioni aziendali e dell'infrastruttura tecnologica, ai sensi di quanto previsto al punto 2, lettera c. del Provvedimento di cui al par. 1.2" che prevede "*gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti da parte del Garante*".

8. LE MODALITÀ DI INFORMAZIONE DEGLI INTERESSATI

Gli interessati sono informati circa l'esistenza delle norme vincolanti d'impresa in modalità differente a seconda della categoria:

Categoria di Interessati	Modalità di comunicazione
Personale di terra subordinato e parasubordinato	Pubblicazione delle *"Norme vincolanti d'impresa"* sulla Intranet aziendale e comunicazione interna a tutto il personale da parte dell'HR Dept. sulla pubblicazione delle norme, con link per la visualizzazione e/o il salvataggio del file in locale.
Personale di bordo	Comunicazione a tutto il personale da parte del Crewing Dept. a mezzo mail con allegate le norme vincolanti e link alla Intranet aziendale. Comunicazione attraverso la newsletter di bordo (Lighthouse).
Candidati	Pubblicazione dell'abstract delle "Norme vincolanti d'impresa sul sito Internet www.damicoship.com, all'interno dell'area riservata per l'invio delle candidature.
Membri degli organi e organismi interni	Pubblicazione delle *"Norme vincolanti d'impresa"* sulla Intranet aziendale e comunicazione interna a tutto il personale da parte dell'HR Dept. sulla pubblicazione delle norme, con link per la visualizzazione e/o il salvataggio del file in locale. Invio a mezzo mail delle "*Norme vincolanti d'impresa*" a tutti i membri degli organi ed organismi interni che non rientrano nella categoria di dipendenti e collaboratori.

9. IL DATA PROTECTION OFFICER (DPO)

In ottemperanza all'art. 37 del Regolamento, DSN, in qualità di Holding del gruppo d'Amico, ha designato un *Data Protection Officer* (o anche 'DPO') unico a livello di gruppo, la Dott.ssa Marzia Vona.

La nomina del DPO è formalizzata attraverso una lettera personalizzata sulla base dei trattamenti effettuati che ne disciplina i compiti.

Il DPO:

- deve essere tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali; deve disporre delle risorse necessarie per assolvere tali compiti e quindi avere a disposizione anche un budget di spesa.
- non è rimosso o penalizzato dal Titolare del trattamento per l'adempimento dei propri compiti.
- riferisce direttamente al vertice gerarchico del Titolare del trattamento.
- può essere contattato dagli Interessati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.
- è tenuto al segreto e/o alla riservatezza in merito all'adempimento dei propri compiti.
- può svolgere altri compiti e funzioni purché non diano adito a un conflitto di interessi.

La direzione del sistema di gestione privacy attraverso tale figura, consentirà al Titolare non solo il rispetto delle prescrizioni in tema di *data protection*, ma anche il controllo dei profili di responsabilità giuridica derivanti dall'applicazione del principio dell'accountability.

Di seguito vengono elencati i principali compiti in capo al DPO:

- coordinare e gestire i Coordinatori privacy nominati dal Titolare del Trattamento per ogni sede del gruppo.

- informare e fornire consulenza a DSN, nonché ai dipendenti che eseguono il trattamento, in merito agli obblighi derivanti dal presente regolamento, nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati.

- sorvegliare l'osservanza del Regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati, nonché delle politiche di DSN 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.

- fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati (o anche *Privacy Impact Assessment*) e sorvegliarne lo svolgimento ai sensi dell'articolo 35.

- cooperare con l'Autorità di Controllo.

- 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.

10. LE PROCEDURE DI RECLAMO

DSN ha impostato una procedura di reclamo da parte degli interessati che si applica a tutte le società del gruppo, che prevede la compilazione di un form da inviare all'attenzione del DPO. Tale form può essere inviato per e-mail o per il tramite dei Coordinatori privacy locali.

I campi del form devono essere compilati in modo dettagliato al fine di consentire al DPO di effettuare le indagini e gli approfondimenti necessari a valutare il reclamo e a proporre le eventuali azioni correttive a DSN.

Il form è disponibile sul sito istituzionale del Gruppo d'Amico al seguente indirizzo: http://www.damicoship.com.

.

11. I MECCANISMI ALL'INTERNO DEL GRUPPO PER GARANTIRE LA VERIFICA DELLA CONFORMITÀ ALLE NORME VINCOLANTI D'IMPRESA

I meccanismi messi in atto da DSN in qualità di Holding del gruppo d'Amico per garantire la verifica della conformità alle norme vincolanti d'impresa comprendono verifiche sulla protezione dei dati e metodi per assicurare provvedimenti correttivi intesi a proteggere i diritti dell'interessato in essere presso le società controllate, di seguito descritti:

- Risk Assessment.
- Privacy Impact Assessment - PIA
- Procedure organizzative.

Il risultato di tali meccanismi di verifica vengono comunicati dal DPO all'organo amministrativo delle società controllate da DSN e resi disponibili su richiesta all'Autorità di controllo competente.

12. I MECCANISMI PER RIFERIRE E REGISTRARE LE MODIFICHE DELLE NORME E COMUNICARLE ALL'AUTORITÀ DI CONTROLLO

Al fine di garantire l'aggiornamento costante verso le Autorità di Controllo delle eventuali modifiche intervenute all'interno delle presenti Norme, DSN in qualità di Holding del gruppo d'Amico seguirà la procedura prevista dalla normativa, con particolare riferimento al CAPO V "*Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali*".

13. LA COOPERAZIONE CON L'AUTORITÀ DI CONTROLLO

DSN, in qualità di Holding del gruppo d'Amico, collabora e coopera con le Autorità di Controllo competenti, fornendo tutto il supporto necessario in caso di esigenze informative, approfondimenti e segnalazioni.

Il DPO designato è il punto di contatto con le Autorità competenti, e garantisce la tempestività di risposta in caso di richieste da parte di suddette Autorità.

14. I MECCANISMI DI SEGNALAZIONE ALL'AUTORITÀ DI CONTROLLO COMPETENTE

DSN, in qualità di Holding del gruppo d'Amico, comunica costantemente, per il tramite del DPO designato, eventuali impatti normativi che potrebbero avere influenza sulle presenti Norme vincolanti di impresa, evidenziando da subito gli elementi rilevanti e le eventuali necessità di aggiornamento delle stesse.

15. LA FORMAZIONE IN MATERIA DI PROTEZIONE DEI DATI AL PERSONALE

Al fine di garantire l'osservanza del Regolamento UE 2016/679, DSN e le società in scope al modello pianificano sessioni formative, con l'obiettivo di sviluppare competenze e capacità in materia di protezione dei dati personali.

In particolare le sessioni sono pianificate dal DPO con il supporto dei Coordinatori privacy e prevedono le seguenti sessioni formative minime su base annuale:

- formazione agli Incaricati.
- formazione ai Responsabili interni.

In aggiunta alle sessioni annuali pianificate, il DPO, con il supporto dei Coordinatori privacy, organizza sessioni formative *ad hoc* in occasione di variazioni organizzative e/o normative rilevanti e sessioni formative dedicate al personale di bordo.

16. ALLEGATI ALLE NORME VINCOLATI D'IMPRESA

ALLEGATO 1 MODELLO PRIVACY DI GRUPPO

Il presente documento si compone di n. 2 sezioni:

- *Sezione I – Executive Summary*, in cui vengono descritti gli obiettivi, le attività realizzate e il modello privacy di gruppo così come definito ad esito delle attività di assessment.
- *Sezione II – Attività realizzate*, in cui vengono descritte le attività di dettaglio realizzate per la definizione del modello di gruppo.

SEZIONE I - EXECUTIVE SUMMARY

I. PREMESSE E OBIETTIVI

Il Gruppo d'Amico, fondato nel 1952, è tra i leader mondiali nel trasporto marittimo nei settori dry cargo e product tankers, e nei servizi strumentali alle attività di *core business*.

Dispone di una tra le più importanti flotte a livello mondiale di navi portarinfuse e navi cisterna. Con uffici in più di 10 sedi nel mondo, il Gruppo d'Amico impiega più di 350 dipendenti e coinvolge circa 3.000 persone a bordo delle navi.

Da sempre il rispetto e la salvaguardia dell'ambiente, l'attenzione al cliente e l'eccellenza professionale del proprio personale rappresentano i capisaldi della propria *mission* e i principi della propria strategia.

d'Amico Società di Navigazione S.p.A., di seguito per brevità DSN, in qualità di Holding del Gruppo imprenditoriale d'Amico, ha avviato, a partire dal 2015, un self assessment della propria organizzazione in ambito privacy ed un assessment privacy presso le sue società controllate con i seguenti obiettivi:

- rilevare, verificare e valutare la corretta applicazione della normativa privacy;
- valutare la fattibilità di un modello privacy a livello di gruppo.

Tale scelta, dettata dall'esigenza di definire una *governance* della privacy a livello Corporate al fine di garantire il rispetto dei diritti degli interessati presso tutte le società del gruppo d'Amico, è stata portata avanti anche negli anni successivi, grazie all'opportunità fornita dal Regolamento 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)*", di seguito per brevità il Regolamento, che ha introdotto il concetto di "gruppo imprenditoriale".

5

II. SINTESI DELLE ATTIVITÀ REALIZZATE

Le attività di assessment sono state condotte attraverso l'analisi della seguente documentazione:

- Regolamento UE 2016/679
- dAmico Organization Chart as of 31 August 2016 - WIP
- dAmico Organization Chart as of 30th June 2016 – FINAL
- Struttura del Gruppo al 30/06/2016 e al 30.06.2017
- Bilanci consolidati al 31/12/2015 e al 31.12.2016 delle società DSN e DIS S.A.
- PRV-01 Registro degli Incaricati Rev.6 16-02-11
- PRV-DPS_Rev8_DSN_DSH_2013_v1_SF_RA
- P-207 Data Protection_rev.2.01
- P-207 Annex 1 Data Protection_rev.2.01
- Documentazione relativa al sistema privacy in essere in DSN (a titolo esemplificativo nomine responsabili interni ed esterni, designazione incaricati del trattamento ed amministratori di Sistema, informative privacy)
- Documentazione relativa al sistema privacy in essere presso le seguenti società controllate: d'Amico International S.A (Lussemburgo), Cogema S.A.M. (Principato di Monaco), d'Amico Shipping UK Ltd (Regno Unito), ISHIMA Pte Ltd (Singapore), d'Amico Shipping USA Limited (Stamford, USA) e d'Amico Dry d.a.c. (Irlanda) (a titolo esemplificativo nomine responsabili

[5]«Gruppo imprenditoriale»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate. *Cfr. Art. 4 "Definizioni", punto 19) del Regolamento UE) 2016/679.*

interni ed esterni, designazione incaricati del trattamento ed amministratori di Sistema, informative privacy).

Si specifica che la scelta di effettuare l'assessment su tali società è stata dettata dalla loro rappresentatività a livello di gruppo.

L'assessment presso le società controllate è stato condotto attraverso la somministrazione di una check list e di interviste con i referenti privacy a livello locale.

Ad esito dell'assessment sulle società controllate è stato prodotto un report di sintesi delle attività, con il dettaglio delle risultanze per ciascuna legal entity.

III. RISULTATI

Le attività di assessment hanno delineato un quadro di sostanziale adeguatezza del rispetto dei requisiti previsti in ambito privacy a livello di normative locali da parte delle società sottoposte a verifica.

Tuttavia, al fine di garantire un ruolo di indirizzo, monitoraggio e controllo da parte di DSN sulle sue controllate in ambito privacy, è stato messo a punto un modello privacy di gruppo che vede DSN e sue controllate in qualità di autonomi titolari del trattamento, con una guida da parte di DSN in riferimento alle policies da seguire all'interno del gruppo per la corretta applicazione della normativa privacy.

Nella "Sezione II" del presente documento sono riportate le attività di dettaglio e i razionali che hanno portato alla definizione del modello privacy di gruppo.

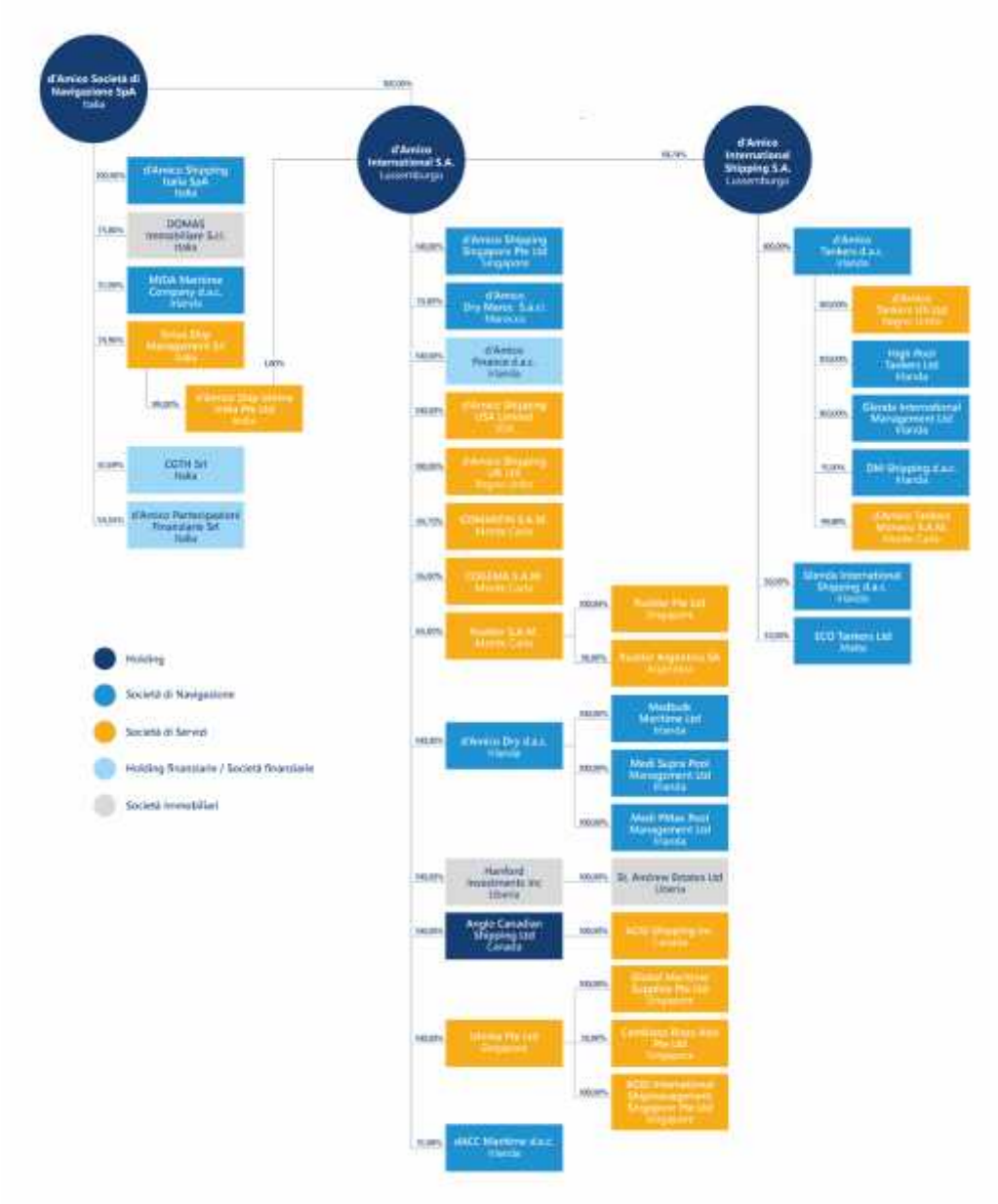
References: : Regolamento (UE) 2016/679 del 27 aprile 2016

SEZIONE II - ATTIVITÀ REALIZZATE

2.1. IL MODELLO PRIVACY DEL GRUPPO D'AMICO

2.1.1 La struttura del Gruppo d'Amico

Si riporta di seguito la struttura del gruppo d'Amico alla data del 30.06.2017.



In particolare, il gruppo d'Amico si compone, alla data del 30.06.2017 di n. 41 società localizzate nei seguenti paesi:

- Italia
- Lussemburgo
- Principato di Monaco
- Regno Unito
- Irlanda
- Malta
- USA
- Canada
- Singapore
- India
- Marocco
- Argentina
- Liberia

Si riporta di seguito l'elenco delle società per paese e per tipologia di attività svolta nell'ambito del gruppo d'Amico:

N.	Società	Paese	Tipologia di società
1	d'Amico Società di Navigazione S.p.A.	Italia	Holding
2	d'Amico Shipping Italia S.p.A.	Italia	Società di navigazione
3	DOMAS Immobiliare S.r.l.	Italia	Società Immobiliare
4	d'Amico Partecipazioni Finanziarie S.r.l.	Italia	Società finanziaria
5	Sirius Ship Management Srl	Italia	Società di servizi
6	CGTH Srl	Italia	Società finanziaria

7	d'Amico International S.A[6].	Lussemburgo	Holding
8	d'Amico International Shipping S.A.	Lussemburgo	Holding
9	d'Amico Tankers Monaco S.A.M.	Principato di Monaco	Società di servizi
10	Cogema S.A.M.	Principato di Monaco	Società di servizi
11	Comarfin S.A.M.	Principato di Monaco	Società di servizi
12	Rudder S.A.M.	Principato di Monaco	Società di servizi
13	d'Amico Dry d.a.c.	Irlanda	Società di navigazione
14	MIDA Maritime Company d.a.c.	Irlanda	Società di navigazione
15	Medbulk Maritime Ltd	Irlanda	Società di navigazione
16	Medi Supra Pool Management Ltd	Irlanda	Società di navigazione
17	Medi PMax Pool Management Ltd	Irlanda	Società di navigazione
18	d'Amico Tankers d.a.c.	Irlanda	Società di navigazione
19	d'Amico Finance d.a.c.	Irlanda	Società finanziaria
20	dACC Maritime d.a.c.	Irlanda	Società di navigazione
21	High Pool Tankers Ltd	Irlanda	Società di navigazione
22	Glenda International Shipping Ltd	Irlanda	Società di navigazione
23	DM Shipping Ltd	Irlanda	Società di navigazione
24	Glenda International Management Ltd	Irlanda	Società di navigazione
25	d'Amico Shipping UK Ltd	Regno Unito	Società di servizi
26	d'Amico Tankers UK Ltd	Regno Unito	Società di servizi
27	ECO Tankers Ltd	Malta	Società di navigazione

[6] Controlla al 50% d'Amico International Shipping S.A.

28	d'Amico Shipping Singapore Pte Ltd	Singapore	Società di navigazione
29	ISHIMA Pte Ltd	Singapore	Società di servizi
30	Global Maritime Supplies Pte Ltd	Singapore	Società di servizi
31	ACGI Pte Ltd	Singapore	Società di servizi
32	Cambiaso Risso Asia	Singapore	Società di servizi
33	Rudder Pte Ltd	Singapore	Società di servizi
34	Anglo Canadian Shipping Ltd	Canada	Holding
35	ACGI Shipping Inc	Canada	Società di servizi
36	d'Amico Ship Ishima India Ltd	India	Società di servizi
37	d'Amico Dry Maroc S.a.r.l.	Marocco	Società di navigazione
38	Rudder Argentina SA	Argentina	Società di servizi
39	d'Amico Shipping USA Limited	USA	Società di servizi
40	Hanford Investments Inc	Liberia	Società immobiliare
41	St. Andrew Estates Ltd	Liberia	Società immobiliare

2.1.2 Le categorie di interessati del gruppo d'Amico

Nel corso delle attività di assessment, oltre alla definizione delle responsabilità delle società all'interno del gruppo, sono state censite e classificate le categorie di interessati per le quali DSN e sue controllate trattano dati personali, che si riportano di seguito:

- Personale di Terra subordinato e parasubordinato e personale di bordo7;

[7] In tale categoria di interessati rientrano tutti i dipendenti a tempo determinato o indeterminato e i Marittimi.

- Candidati e Colloquiandi;
- Clienti e Prospect;
- Fornitori8;
- Visitatori;
- Componenti degli Organi e Organismi interni di D'Amico (OdV, Collegio Sindacale e CdA);

Per ciascuna categoria di interessati sono state rilevate e classificate le seguenti informazioni, che sono riportate nel dettaglio all'interno del documento "*Registro delle attività di trattamento del gruppo d'Amico*", disponibile presso la Holding DSN e sue controllate per tutte le categorie di interessati e per le Autorità di Controllo:

Categoria di dati: indica la categoria di dati gestiti per ciascuna categoria di interessati (art.30, comma 1, lettera c) del Regolamento).

Base giuridica del Trattamento: la base giuridica del trattamento è costituita, per le categorie di interessati riferite a Dipendenti, Collaboratori, Candidati e Membri degli Organi ed Organismi interni di DSN, dall'Articolo 9, lettere a) e b) del Regolamento, che si riportano di seguito:

a. 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 al trattamento dei dati personali di tipo sensibile previsto al medesimo articolo del Regolamento;

b. 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

[8] In tale categoria di interessati rientrano anche i Professionisti Esterni.

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.

La base giuridica del trattamento è costituita, per le categorie di Interessati riferite Fornitori e Clienti e Prospect, dall'Articolo 6, lettere b) e c) del Regolamento, che si riportano di seguito:

b. 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;

c. il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento.

Finalità del trattamento: indica le motivazioni o le attività inerenti allo specifico trattamento dei dati (art. 30, comma 1, lettera b) del Regolamento).

Repository: indica il nome dell'applicativo (nel caso in cui l'archiviazione è effettuata in modalità elettronica) o dell'archivio cartaceo (nel caso in cui l'archiviazione è effettuata in modalità cartacea) utilizzato per la gestione dei dati relativi a ciascuna classe di Interessati. Tra gli applicativi sono esclusi i documenti di lavoro (es. file MS Excel) lavorati dalle risorse, che riportano al loro interno dati personali acquisiti da altri software aziendali.

Categorie di destinatari che concorrono al trattamento: indica la Società/Struttura interna o esterna al Titolare, compresi i destinatari di paesi terzi od organizzazioni internazionali, a cui i dati personali sono stati o saranno comunicati (art. 30, comma 1, lettera d) del Regolamento).

Alla luce del quadro sopra delineato, e in riferimento a quanto previsto dal Regolamento in tema di gruppi imprenditoriali[9], è stata effettuata la declinazione del modello privacy sulla struttura del Gruppo d'Amico.

Il primo passo per la declinazione del modello privacy è stato quello di definire il perimetro delle società ricadenti nel modello (*in scope* e *out of scope* al modello).

Tale attività è stata realizzata utilizzando il criterio principale della "influenza dominante" esercitata da DSN sulle società controllate.

Il concetto di influenza dominante è stato mutuato dal Considerando n. 37 del Regolamento n. 679/2016, di seguito riportato:

"*Un gruppo imprenditoriale dovrebbe costituirsi di un'impresa controllante e delle sue controllate, là dove l'impresa controllante dovrebbe essere quella che può esercitare un'influenza dominante sulle controllate in forza, ad esempio, della proprietà, della partecipazione finanziaria o delle norme societarie o del potere di fare applicare le norme in materia di protezione dei dati personali*".

In forza di tale definizione, è stata effettuata una prima classificazione delle società, secondo la suddivisione in società *"in scope"* e *"out of scope"* al modello.

A seguito di questa prima classificazione, si è proceduto con l'applicazione di un secondo criterio, relativo al *core business* delle società *out of scope*, per verificare se fosse opportuno far rientrare all'interno del modello anche quelle società che, seppur in assenza di uno o più dei criteri enunciati dal Regolamento, si configurano come "*società di navigazione*".

Al termine di questa riclassificazione, si è proceduto all'analisi dei risultati e alla ponderazione degli stessi attraverso l'applicazione di criteri natura più soggettiva per gestire situazioni "*specifiche*", quali ad esempio la presenza, all'interno delle società risultanti dalla riclassificazione come *out of scope* al modello, di personale dipendente in forza a società *in scope* al modello.

9.*Cfr. Considerando n. 37 del Regolamento.*

Alla luce di questo ulteriore criterio di ponderazione è stato delineato il perimetro definitivo delle società *in scope* e *out of scope* al modello privacy, di cui si riportano di seguito i razionali in termini di ruoli e responsabilità della Holding e delle controllate.

- Società *in scope* al modello: tali società sono inquadrate all'interno del modello privacy in qualità di autonomi Titolari del trattamento all'interno del gruppo.

  Per queste società DSN eserciterà il ruolo di indirizzo, monitoraggio e controllo in materia di privacy, potendo esercitare un'influenza dominante in forza dei criteri enunciati sopra. Tale ruolo si esplicherà fornendo il supporto necessario in termini di assistenza, consulenza e framework documentale comune.

- Società *out of scope* al modello: tali società sono inquadrate all'interno del modello in qualità di autonomi Titolari del trattamento al di fuori del gruppo.

  Per queste società DSN non eserciterà il ruolo di indirizzo in materia di privacy, fermo restando il controllo sull'operato delle stesse in qualità di società rientranti all'interno del gruppo d'Amico e il supporto su richiesta da parte delle società controllate.

Si riporta di seguito l'elenco delle società così come riclassificato alla luce delle attività di assessment:

- n. 32 società del gruppo in qualità di autonomi titolari del trattamento all'interno del modello (*in scope* al modello)

N.	Società	Paese	Tipologia di società
1	d'Amico Società di Navigazione S.p.A.	Italia	Holding
2	d'Amico Shipping Italia S.p.A.	Italia	Società di navigazione
3	Sirius Ship Management Srl	Italia	Società di servizi
4	d'Amico International S.A[1].	Lussemburgo	Holding
5	Cogema S.A.M.	Principato di Monaco	Società di servizi
6	Comarfin S.A.M.	Principato di Monaco	Società di servizi
7	d'Amico Dry d.a.c.	Irlanda	Società di navigazione
8	Medbulk Maritime Ltd	Irlanda	Società di navigazione
9	Medi PMax Pool Management Ltd	Irlanda	Società di navigazione
10	d'Amico Shipping UK Ltd	Regno Unito	Società di servizi
11	d'Amico Shipping Singapore Pte Ltd	Singapore	Società di navigazione
12	d'Amico International Shipping S.A.	Lussemburgo	Holding
13	d'Amico Tankers Monaco S.A.M.	Principato di Monaco	Società di servizi
14	d'Amico Ship Ishima India Ltd	India	Società di servizi
15	d'Amico Shipping USA Limited	USA	Società di servizi
16	Hanford Investments Inc	Liberia	Società immobiliare
17	St. Andrew Estates Ltd	Liberia	Società immobiliare
18	d'Amico Tankers d.a.c.	Irlanda	Società di navigazione
19	dACC Maritime d.a.c.	Irlanda	Società di navigazione
20	High Pool Tankers Ltd	Irlanda	Società di navigazione
21	Glenda International Shipping Ltd	Irlanda	Società di navigazione
22	DM Shipping Ltd	Irlanda	Società di navigazione
23	Glenda International Management Ltd	Irlanda	Società di navigazione
24	d'Amico Tankers UK Ltd	Regno Unito	Società di servizi
25	MIDA Maritime Company d.a.c.	Irlanda	Società di navigazione
26	d'Amico Dry Maroc S.a.r.l.	Marocco	Società di navigazione
27	Medi Supra Pool Management Ltd	Irlanda	Società di navigazione
28	ISHIMA Pte Ltd	Singapore	Società di servizi
29	ACGI Pte Ltd	Singapore	Società di servizi

30	Anglo Canadian Shipping Ltd	Canada	Holding
31	ACGI Shipping Inc	Canada	Società di servizi
32	DOMAS Immobiliare S.r.l.	Italia	Società Immobiliare

- n. 9 società del gruppo in qualità autonomi titolari del trattamento, al di fuori del modello (*out of scope* al modello)

N.	Società	Paese	Tipologia di società
1	d'Amico Partecipazioni Finanziarie S.r.l.	Italia	Società finanziaria
2	CGTH Srl	Italia	Società finanziaria
3	ECO Tankers Ltd	Malta	Società di navigazione
4	Cambiaso Risso Asia Pte Ltd	Singapore	Società di servizi
5	Rudder Argentina SA	Argentina	Società di servizi
6	d'Amico Finance d.a.c.	Irlanda	Società finanziaria
7	Rudder S.A.M.	Principato di Monaco	Società di servizi
8	Rudder Pte Ltd	Singapore	Società di servizi
9	Global Maritime Supplies Pte Ltd	Singapore	Società di servizi

2.1.3 Ruoli e responsabilità in ambito privacy

A completamento della definizione del modello privacy di gruppo sono stati definiti i seguenti ruoli e responsabilità:

- Titolari del Trattamento: DSN e tutte le società controllate *in scope* al modello sono autonomi Titolari del trattamento dei dati per le categorie di interessati riportate al paragrafo 1.2. "Le categorie di interessati del gruppo d'Amico".

  Come già esplicitato sopra, per queste società DSN esercita il ruolo di indirizzo, monitoraggio e controllo, in qualità di Holding, per la corretta applicazione delle regole per la gestione della privacy definite a livello Corporate.

- Responsabili interni del trattamento: DSN e le società *in scope* al modello che presentano una complessità organizzativa maggiore in funzione del numero di dipendenti, in qualità di autonomi Titolari del Trattamento, hanno nominato in qualità di Responsabili interni del Trattamento dei dati, i Responsabili delle Funzioni Organizzative, che nell'ambito delle proprie attribuzioni, trattano manualmente o con strumenti elettronici, dati personali di cui DSN e le società *in scope* sono Titolari.
- Incaricati interni del Trattamento: DSN e le società *in scope* al modello, in qualità di autonomi Titolari del Trattamento, hanno individuato differenti Classi di Incaricati nelle quali rientrano tutti i dipendenti e collaboratori delle varie società del Gruppo che, nell'ambito delle proprie mansioni, trattano manualmente o con strumenti elettronici, dati personali di cui DSN e le società *in scope* sono Titolari.
- Responsabili esterni del Trattamento:

  DSN e tutte le società *in scope* e *out of scope* al modello sono Responsabile Esterni del trattamento dei dati per le altre società del gruppo (ciascuna società è Responsabile esterno del trattamento per tutte le altre), a prescindere dai contratti commerciali infragruppo in essere. Tale scelta è motivata dal fatto che non è possibile escludere che, al di fuori degli accordi commerciali formalizzati, possa configurarsi comunque un eventuale transito di dati personali riferiti agli interessati.

  Tutte le società e i professionisti che forniscono servizi alle singole società del gruppo *in scope* al modello, che nell'ambito dell'incarico ricevuto trattano manualmente o con strumenti elettronici, dati personali di cui DSN e le società *in scope* sono Titolari.
- Data Protection Officer (DPO): in ottemperanza all' art. 37 del Regolamento, DSN ha designato quale Responsabile della Protezione dei dati a livello di gruppo, in staff al Titolare del Trattamento di DSN, la Dott.ssa Marzia Vona.

- Coordinatori privacy: DSN, al fine di agevolare il coordinamento e la gestione delle azioni volte al rispetto del Regolamento, ha nominato, per ogni country del gruppo a livello internazionale, un Coordinatore Privacy.

ALLEGATO 2 RISK ASSESSMENT

2.1. Estratto dall'Analisi dei rischi

La metodologia di riferimento utilizzata è riconducibile alla Linee Guida dei principali standard internazionali per il Risk Assessment e la sicurezza dei sistemi informativi (ISO 27001:2005 e la ISO 27005), e si pone l'obiettivo di produrre risultati comparabili e riproducibili nel tempo.

Le fasi metodologiche previste dagli standard, che sono state seguite per la realizzazione delle attività, sono le seguenti:

- identificazione dei rischi.
- analisi e valutazione dei rischi.

Si riporta di seguito il dettaglio delle relative fasi metodologiche.

2.1.1. Identificazione dei Rischi

L'identificazione dei rischi avviene attraverso un procedimento strutturato che pone il focus sulle risorse da proteggere.

Tale fase si articola nelle seguenti quattro sotto-fasi:

1. identificazione delle risorse;
2. identificazione degli eventi dannosi e dei fattori di rischio;
3. classificazione dei rischi;
4. rilevazione delle misure di sicurezza esistenti.

Di seguito il dettaglio degli obiettivi e delle attività di ciascuna sotto-fase.

2.1.1.1. Identificazione delle risorse

La sotto-fase permette di individuare tutte le risorse informative delle Società, i dati personali gestiti e i relativi trattamenti oggetto dell'analisi. Le informazioni sono acquisite tramite la realizzazione di interviste effettuate ai referenti di ciascuna struttura interessata.

2.1.1.2. Identificazione degli eventi dannosi e dei fattori di rischio

La sotto-fase consente di identificare, per ciascuna delle risorse precedentemente individuate, tutti gli eventi dannosi in grado di compromettere i requisiti di integrità, confidenzialità, disponibilità e affidabilità dei dati personali. Successivamente, per ciascun evento, vengono identificati i fattori di rischio, ovvero le modalità con cui gli eventi dannosi possono manifestarsi per ciascuna risorsa in esame.

L'identificazione di eventi dannosi e fattori di rischio avviene considerando sia la specificità dell'organizzazione e dell'infrastruttura della Società, sia le indicazioni fornite dall'Autorità di Controllo.

2.1.1.3. Classificazione dei Rischi

La sotto-fase consente di definire le macro categorie di rischi oggetto dell'analisi, come di seguito riportate:

- Rischi inerenti i sistemi informativi e la sicurezza dei dati, a loro volta distinti in:
  - Rischi fisici: rischi relativi alle aree e locali dove sono disposti i sistemi e i dispositivi di comunicazione, rischi relativi all'accesso di persone nei locali medesimi, rischi relativi all'integrità e disponibilità dei sistemi e dispositivi ICT (mancanza di protezione dei locali, mancanza di controllo degli accessi ecc.).
  - Rischi logici: rischi relativi all'integrità, riservatezza e disponibilità dei dati.
  - Rischi di trasmissione: rischi relativi alla sicurezza delle trasmissioni dei dati.
- Rischi di Compliance: rischi relativi al mancato rispetto dei diversi adempimenti previsti dal Regolamento (es. nomine responsabili e incaricati dei trattamenti, predisposizione informative e relative richieste di autorizzazione ai trattamenti, formazione ecc.).

2.1.1.4. Rilevazione delle misure di sicurezza esistenti

La sotto-fase consente di individuare le misure di protezione esistenti per la mitigazione dei rischi. In tal senso è necessario tenere conto sia delle misure di sicurezza informatiche, sia delle misure di sicurezza fisiche ed organizzative.

2.2.1. Analisi e valutazione dei rischi

Nel corso di questa fase viene effettuata la misurazione del cosiddetto "livello di rischio residuo", con cui si intende il rischio residuo valutato dopo aver effettuato la valutazione del sistema di controllo e delle azioni intraprese per mitigare il rischio inerente. Tale fase si realizza attraverso le seguenti tre sotto-fasi:

1. determinazione del livello di rischio inerente
2. determinazione del livello di rischio residuo
3. identificazione e valutazione delle opzioni per il trattamento dei rischi

2.2.1.1. Determinazione del livello di rischio inerente

Il rischio inerente è generalmente definito come il rischio connesso ad una attività e/o a un processo aziendale, a prescindere dal livello di controllo presente nello stesso.

I fattori che determinano il livello di rischio inerente sono l'impatto, ovvero la rilevanza delle conseguenze causate dall'evento dannoso e la probabilità, ovvero la possibilità che l'evento dannoso si verifichi in un periodo di riferimento.

Le tabelle 1 e 2 riportano, rispettivamente, i valori di impatto e probabilità assegnati nella valutazione.

Tabella 1 - Assegnazione dei Valori di impatto

Impatto	Indice	Significato
Basso	10	Gli effetti dell'evento dannoso sono limitati sotto ogni punto di vista: legale, funzionale e di reputazione.
Medio	50	Gli effetti dell'evento dannoso sono circoscritti, con conseguenze significative ma sostenibili.
Alto	100	Gli effetti dell'evento dannoso possono comportare gravi conseguenze per l'organizzazione.

Tabella 2 - Assegnazione dei Valori di probabilità

Probabilità	Indice	Significato
Basso	0,1	L'evento potrebbe verificarsi al massimo una volta in un arco temporale maggiore di 10 anni.

Medio	0,5	L'evento potrebbe verificarsi più volte nell'arco temporale di 10 anni, ma non annualmente.
Alto	1	L'evento potrebbe verificarsi almeno una volta nell'arco di un anno.

L'entità del rischio inerente è data, quindi, dalla relazione tra la probabilità di accadimento dell'evento e l'impatto negativo potenziale generato.

Le tabelle 3 e 4 riportano rispettivamente la valutazione e descrizione del rischio inerente.

Tabella 3 – Valutazione del rischio inerente

Livello di Rischio		Probabilità		
		Bassa	Media	Alta
Impatto	Basso	1	5	10
	Medio	5	25	50
	Alto	10	50	100

Tabella 4 - Descrizione del rischio inerente

Livello di rischio	Valore	Significato
Basso	< 10	Il livello di rischio inerente è trascurabile e non è necessario predisporre misure di controllo.
Medio	>= 10 e < 50	Il livello di rischio inerente non è trascurabile, ed è opportuno predisporre misure di controllo per la mitigazione del rischio.
Alto	>= 50	Il livello di rischio inerente è elevato, ed è necessario predisporre misure di controllo per la mitigazione del rischio.

2.2.1.2. Determinazione del livello di rischio residuo

Il rischio residuo o mitigato è generalmente definito come il rischio che rimane in seguito alla valutazione del sistema di controllo. L'entità di tale rischio si determina attraverso la combinazione di entità del rischio inerente e valutazione di adeguatezza dei controlli (o misure di protezione) in essere, come riportato nella Tabella 5.

Tabella 5 - Determinazione del rischio residuo

Rischio Residuo		Valutazione controlli		
		Adeguato	Parziale	Non Adeguato
Rischio Inerente	Basso	Basso	Basso	Medio
	Medio	Basso	Medio	Alto
	Alto	Medio	Alto	Alto

2.2.1.3. Identificazione e valutazione delle opzioni per il trattamento dei rischi

Al termine di sotto-fase, laddove si riscontri un livello di rischio residuo medio o alto, è possibile identificare ulteriori misure di sicurezza, al fine di ricondurre il rischio ad un livello di accettabilità.

Tra le opzioni disponibili, è possibile accettare i rischi consapevolmente e obiettivamente, nel rispetto delle politiche aziendali. In alternativa si potrà decidere se evitare il rischio, annullando il fattore di rischio o rinunciando ad una determinata risorsa.

Da ultimo, sarà possibile decidere di trasferire il rischio ad altro soggetto, ad esempio a un'assicurazione o a un fornitore.

2.2.2. Risultati dell'Analisi

Nei paragrafi successivi sono riportati i risultati dell'analisi dei rischi realizzata.

2.2.2.1. Identificazione dei rischi

Per procedere all'identificazione dei rischi è stata esaminata l'organizzazione e l'infrastruttura dei Sistemi Informativi del gruppo d'Amico, che si riporta di seguito.

2.2.2.1.1. Rilevazione dell'infrastruttura tecnologica e applicativa

La gestione dell'infrastruttura ICT del gruppo d'Amico è demandata al provider Virtustream con sede a Londra, ed è regolata da un contratto IaaS (Infrastructure-as-a-Service). In aggiunta, alcune attività critiche sono gestite in SaaS (Software-as-a-Service).

Di seguito si elencano i principali server ospitati nel Data Center di Londra (UK-DC) del provider informatico:

- domain controller;
- file server;
- server dati e applicazioni;
- server di posta elettronica;
- server di backup;
- sftp server.

Tutte le macchine virtuali ospitate nel Data Center Virtustream di Londra (UK-DC) sono ridondate nel Data Center Virtustream di Amsterdam (NL-DC).

La connessione con i server d'Amico è garantita da una linea MPLS, gestita da fornitori esterni, che articola le seguenti sedi del gruppo: Roma, Genova, Dublino, Monaco, Singapore, Lussemburgo, Londra, Stamford, Mumbai, Manila, ed è ridondata mediante l'utilizzo di una linea di Backup.

La connessione alla rete telematica avviene tramite *firewall* che monitorano costantemente il traffico Internet in entrata e in uscita con lo scopo di:

- gestire gli accessi ad Internet e registrare i log di navigazione;

- controllare il traffico web;
- Antivirus;
- Anti-Spyware.

Le workstation ubicate presso le sedi d'Amico sono collegate alla LAN aziendale, permettendo l'utilizzo di unità di rete ad accesso limitato al personale appartenente ai Dipartimenti Aziendali, segregazioni ad accesso limitato ai singoli dipendenti e unità di rete per lo scambio documentale.

Sui server e sui client è installato un antivirus configurato in modo da essere continuamente e automaticamente aggiornato su ogni singolo client con le ultime release della casa produttrice. Gli utenti non possono bloccare o annullare l'aggiornamento e la scansione della ricerca di virus.

La figura 1 riporta l'articolazione dell'infrastruttura tecnologica del gruppo d'Amico:

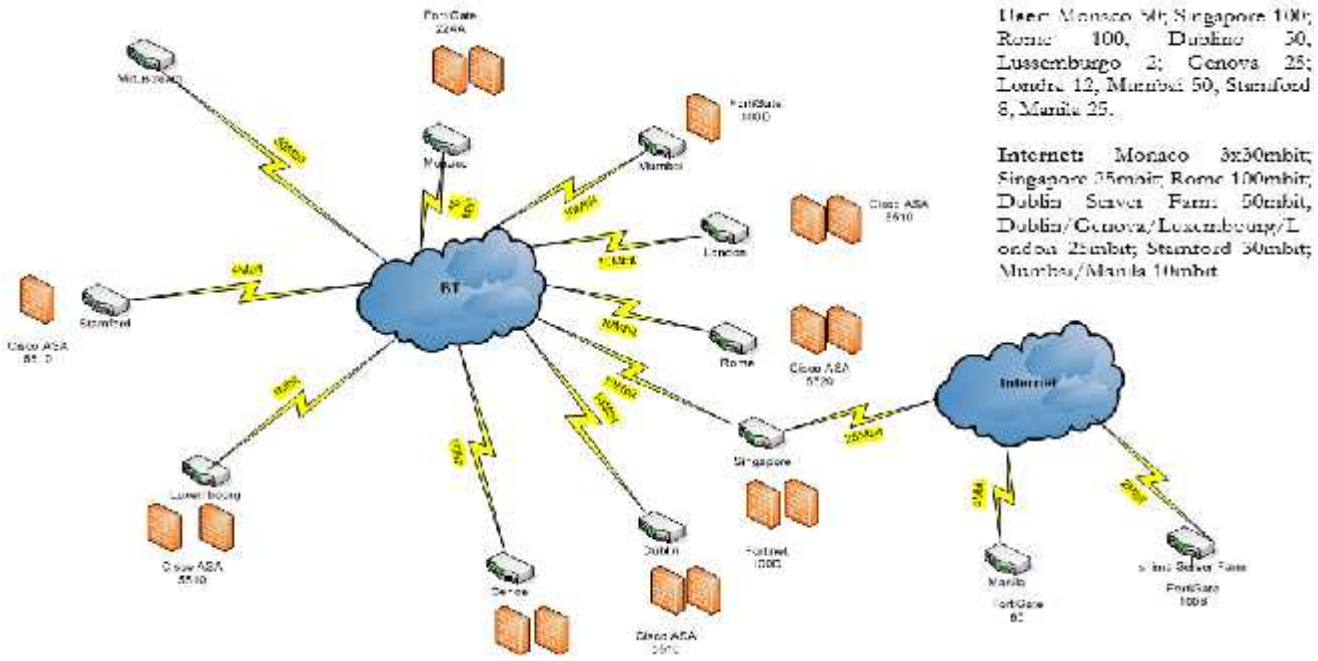


Figura 1 – Articolazione infrastruttura tecnologica d'Amico Group

Gli applicativi e le relative basi di dati presenti in d'Amico, che rientrano nel campo di applicazione del Regolamento, sono dettagliati nel file "Infrastrutture e applicazioni ICT DAMICO_IT".

2.2.2.1.2. Principali rischi e relative misure di sicurezza

Le tabelle seguenti riportano i principali eventi dannosi per la sicurezza dei dati e la valutazione delle possibili conseguenze e della gravità, in relazione ai seguenti contesti e strumenti elettronici utilizzati:

- Backup dei dati;
- Comportamento degli operatori;
- Gestione incident;
- Raccolta di log e monitoraggio;
- Sicurezza fisica;
- Sicurezza Data Center di gruppo;
- Sicurezza logica degli accessi;
- Sicurezza dei dati;
- Sicurezza della rete;
- Sicurezza degli applicativi;
- Sicurezza logica;
- Sicurezza workstation.

2.2.2.2. Valutazione dei rischi

Matrice dei rischi

Contesto	Evento	Fattore di Rischio	Impatto	Probabilità	Rischio Inerente	Misura di protezione in essere	Valutazione dei controlli	Rischio Residuo
Backup dei dati	Asportazione e furto dei back up	- Inadeguatezza luogo di conservazione	M	B	B	- WI-ITG-02 Back-up Quick Reference - Backup Virtustream	Adeguato	Basso
Backup dei dati	Distruzione e perdita dati	- Indisponibilità dei dati	M	M	M	- SLA di Contratto	Parziale	Medio
Backup dei dati	Contenzioso con fornitore	- Indisponibilità dei dati	A	B	M	- SLA di Contratto	Parziale	Medio
Comportamento degli operatori	Accessi non autorizzati ai sistemi aziendali	- Inadeguatezza dei sistemi di autenticazione	B	B	B	- Adozione di regole di Strong Authentication - ITG-01 Acceptable use of ICT Resources Policy	Adeguato	Basso
Comportamento degli operatori	Perdita dei dati contenuti nei sistemi aziendali	- Carenza di consapevolezza, incuria, disattenzione da parte dei dipendenti	B	B	B	- Back up giornalieri - ITG-01 Acceptable use of ICT Resources Policy - PIM	Adeguato	Basso
Comportamento degli operatori	Furto di strumenti contenenti dati	- Omessa custodia	B	B	B	- Codice Etico - PIM	Adeguato	Basso

Contesto	Evento	Fattore di Rischio	Impatto	Probabilità	Rischio Inerente	Misura di protezione in essere	Valutazione dei controlli	Rischio Residuo
Gestione incident	Malfunzionamento, indisponibilità delle applicazioni	- Inadeguato monitoraggio	M	M	M	- ITG-07 ERP Emergency Change	Parziale	Medio
Monitoraggio dei sistemi	Malfunzionamento, indisponibilità delle applicazioni	- Inadeguata rilevazione delle eccezioni, dei malfunzionamenti e degli eventi relativi ai sistemi	M	B	B	- ITG-07 ERP Emergency Change	Adeguato	Basso
Raccolta di log e monitoraggio	Manomissione log	- Inadeguatezza dei sistemi di autenticazione in cui risiedono i log	B	B	B	- Adozione di regole di Strong Authentication - ITG-01 Acceptable use of ICT Resources Policy	Adeguato	Basso
Raccolta di log e monitoraggio	Comportamenti fraudolenti da parte degli Amministratori di Sistema	- Inadeguato monitoraggio sull'operato degli Amministratori di Sistema	A	B	M	- Monitoraggio semestrale degli access log degli Amministratori di sistema - Codice Etico	Parziale	Medio
Sicurezza fisica	Accessi non autorizzati agli edifici di proprietà aziendale	- Assenza di misure di protezione ambientale nelle aree che contengono informazioni sensibili o critiche - Errori umani nella gestione della sicurezza fisica	M	B	B	- Presidio degli uffici - Registrazione degli ingressi (ove applicabile) - Servizio di Portineria (ove applicabile)	Adeguato	Basso
Sicurezza fisica	Accessi non autorizzati ai reparti ad accesso ristretto	- Inadeguatezza nella gestione degli accessi ai reparti ad accesso ristretto (ex. CED)	M	B	B	- Badge (ove applicabile)	Adeguato	Basso

Contesto	Evento	Fattore di Rischio	Impatto	Probabilità	Rischio Inerente	Misura di protezione in essere	Valutazione dei controlli	Rischio Residuo
		- Violazione sistemi antiintrusione				- Codice Etico - Porte chiuse a chiave (ove applicabile)		
Sicurezza fisica	Minacce esterne ed ambientali che potrebbero provocare un indisposizione delle apparecchiature	- Inadeguata protezione fisica da calamità naturali, attacchi malevoli o accidenti	M	B	B	- Antivirus (centralizzato) - Firewall - Disaster Recovery Plan - Gruppo di continuità - Ridondanza dei Server in cui risiedono le applicazione e i dati	Adeguato	Basso
Sicurezza Data Center di gruppo (cfr. contratto fornitura Virtustream)	Eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria	- Mancanza di misure di protezione ambientale - Mancanza misure di continuità	B	B	B	SLA di Contratto Virtustream	Adeguato	Basso
Sicurezza Data Center di gruppo	Guasto ai sistemi complementari (impianto elettrico, climatizzazione, …)	- Mancanza di sistemi di alimentazione - Surriscaldamento apparecchiature	B	B	B	- Manutenzione periodica degli impianti - Gruppo di continuità	Adeguato	Basso
Sicurezza Data Center di gruppo	Errori umani nella gestione della sicurezza fisica	- Carenza di consapevolezza, incuria, disattenzione	B	B	B	- Policy di Gruppo - Formazione interna - Sistema disciplinare	Adeguato	Basso
Sicurezza logica degli accessi	Accesso ai dati da parte di personale non autorizzato	- Assenza di un processo per l'assegnazione o la revoca dei diritti di accesso per tutte le	M	B	B	- ITG-09 User Accounts - Monitoraggio dei tentativi di accesso falliti	Adeguato	Basso

Contesto	Evento	Fattore di Rischio	Impatto	Probabilità	Rischio Inerente	Misura di protezione in essere	Valutazione dei controlli	Rischio Residuo
		tipologie di utenze e per tutti i sistemi e server in linea con la posizione ricoperta - Assenza di una politica di controllo degli accessi						
Sicurezza logica degli accessi	Perdita di riservatezza della password di accesso ai sistemi	- Inadeguato livello di sicurezza della Password	B	B	B	- ITG-09 User Accounts - Adozione di regole di Strong Authentication in linea con le best practices internazionali (>8 caratteri; alfanumerica, non deve correlata a informazioni personali (ex nome ad esempio, la data di nascita, ecc.), cambio password ogni 90gg	Adeguato	Basso
Sicurezza dei dati	Furto di dati	- Carenza di consapevolezza, incuria, disattenzione	B	B	B	- Dati crittografati sia in storage clouds sia in rete	Adeguato	Basso
Sicurezza dei dati	Accesso non autorizzato ai dati da parte del Fornitore Virtustream	- Assenza di una policy sull'uso, sulla protezione e sulla durata delle chiavi crittografiche	M	B	B	- Cifratura dei dati personali	Adeguato	Basso
Sicurezza della rete	Perdita dei dati di rete	- Mancanza copie di sicurezza	M	B	B	- WI-ITG-02 Back-up Quick Reference -Backup giornalieri	Adeguato	Basso
Sicurezza della rete	Attacco Virus, Worm, Malware	- Mancanza di software di contrasto dei codici malevoli	M	B	B	- Firewall - Antivirus - Antispam	Adeguato	Basso

Contesto	Evento	Fattore di Rischio	Impatto	Probabilità	Rischio Inerente	Misura di protezione in essere	Valutazione dei controlli	Rischio Residuo
						- Ridotti privilegi per gli utenti		
Sicurezza della rete	Errore di elaborazione	- Errata gestione, modifica o aggiornamento programmi	M	B	B	- Ambiente di test separato da Ambiente di produzione - Test preliminare degli aggiornamenti o modifiche evolutive - PO Change	Adeguato	Basso
Sicurezza degli applicativi	Malfunzionamento, indisponibilità o degrado delle apparecchiature	- Architettura di rete con ridotta affidabilità - Mancato aggiornamento	B	B	B	- Ridondanza dei server - Aggiornamento periodico dei server di infrastruttura - Macchine virtuali	Adeguato	Basso
Sicurezza degli applicativi	Accesso non autorizzato a sistema informativo	- Inadeguatezza sistemi di autenticazione	B	B	B	- Credenziali di accesso - ITG-01 Acceptable use of ICT Resources Policy	Adeguato	Basso
Sicurezza degli applicativi	Attacco Virus, Worm, Malware	- Mancanza di software di contrasto dei codici malevoli	M	B	B	- Firewall - Antivirus - Antispam - Ridotti privilegi per gli utenti	Adeguato	Basso
Sicurezza degli applicativi	Furto o perdita di dati	- Apparecchiature incustodite degli utenti	B	B	B	- ITG-01 Acceptable use of ICT Resources Policy - Sicurezza perimetrale degli Uffici	Adeguato	Basso

Contesto	Evento	Fattore di Rischio	Impatto	Probabilità	Rischio Inerente	Misura di protezione in essere	Valutazione dei controlli	Rischio Residuo
Sicurezza logica	Azione di virus informatici o di programmi suscettibili di provocare danno	- Mancanza di software di contrasto dei codici malevoli	A	M	A	- Antivirus - Penetration test	Adeguato	Medio
Sicurezza logica	Spamming o tecniche di sabotaggio	- Insufficienti di policy di sicurezza	B	B	B	- Antispam - ITG-01 Acceptable use of ICT Resources Policy	Adeguato	Basso
Sicurezza logica	Malfunzionamento, degrado o indisponibilità delle applicazioni	- Mancato aggiornamento	B	B	B	- Aggiornamento periodico dei SW	Adeguato	Basso
Sicurezza logica	Accessi esterni non autorizzati	- Inadeguatezza dei sistemi di autenticazione	B	B	B	- Adozione di regole di Strong Authentication - ITG-01 Acceptable use of ICT Resources Policy	Adeguato	Basso
Gestione degli asset	Furto e perdita dei dati	Data Disclosure	M	B	B	- Crittografia dei supporti magnetici	Adeguato	Basso
Sicurezza workstation	Installazione di software o dispositivi atti al sabotaggio o all'intercettazione delle informazioni	- Insufficienti di policy di sicurezza	B	B	B	- Antispam - ITG-01 Acceptable use of ICT Resources Policy	Adeguato	Basso
Sicurezza workstation	Distruzione e perdita dati	- Mancanza di copie di sicurezza	B	B	B	- WI-ITG-02 Back-up Quick Reference	Adeguato	Basso

References: : Regolamento (UE) 2016/679 del 27 aprile 2016

2.3. Considerazioni conclusive

Dall'analisi effettuata emerge un quadro complessivo di sostanziale adeguatezza del sistema dei controlli in essere all'interno del gruppo d'Amico, che garantisce una tutela adeguata dei dati personali, in linea con le prescrizioni del Regolamento 679/2016.

L'analisi ha evidenziato, tuttavia, alcune aree di miglioramento sulle quali si raccomanda di intervenire.

In relazione a "Backup dei dati", "Gestione incident" e "Raccolta di Log e Monitoraggio" il gruppo d'Amico ha predisposto una risposta al rischio residuo, al fine di ridurlo, pianificando le seguenti azioni:

- revisione delle procedure di Back-up, Configurazioni IS, disaster recovery.
- sicurezza dei dati riferiti ai documenti On Shore e On Board;
- monitoraggio dei Log di Incident Database e degli Incident Workaround.
- raccolta log e monitoraggio semestrale degli access log degli Amministratori di sistema
- impostazione delle clausole di sicurezza contrattuali con fornitori di terze parti

In relazione alla "Sicurezza Logica", il gruppo d'Amico ha accettato il relativo rischio residuo.

2.4. Documenti di riferimento

- ✓ ICT Governance:
  - ITG-01 Acceptable use of ICT Resources Policy V.2.01;
  - ITG-02 Global ICT Security Policy;
  - ITG-07 ERP Emergency Change;
  - ITG-09 Users Accounts;
  - ITG-10 Backup;
  - ITG-11 IS Configurations;
  - WI-ITG-02 Back-up Quick Reference;
  - WI-ITG-03 Competence Chart;
  - WI-ITG-04 Users Authorization register;
  - Disaster Recovery Plan.
- ✓ Corporate Governance:

- Code of Ethics;
- 231 Model;
- Social Media Policy.

References: : Regolamento (UE) 2016/679 del 27 aprile 2016