REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO DEL GRUPPO D'AMICO

Issued	*Approved*
Data Protection Officer	*HR Department*

Distribution

Tutti i Responsabili e gli Incaricati del Trattamento Dati Personali

INDICE

1. PREMESSE ---------- 3

1.1. CONTESTO DI RIFERIMENTO: NORMATIVA E ASSUMPTIONS ---------- 3
1.2. PRINCIPALI DEFINIZIONI ---------- 4
1.3. OBIETTIVI DEL DOCUMENTO ---------- 7
1.4. STRUTTURA DEL DOCUMENTO ---------- 8
1.5. CONSERVAZIONE DEL DOCUMENTO ---------- 8
1.6. AMBITO DI DISTRIBUZIONE INTERNA DOCUMENTO ---------- 8
1.7. AGGIORNAMENTO DEL DOCUMENTO ---------- 9
1.8. RESPONSABILE DELL'AGGIORNAMENTO DEL DOCUMENTO ---------- 9

2. IL MODELLO PRIVACY DEL GRUPPO D'AMICO ---------- 10

2.1. LA STRUTTURA DEL GRUPPO D'AMICO ---------- 10
2.2. LE CATEGORIE DI INTERESSATI DEL GRUPPO D'AMICO ---------- 12
2.3. RUOLI E RESPONSABILITA' IN AMBITO PRIVACY ---------- 26

3. L'ANALISI DEI RISCHI (ART.32) ---------- 31

3.1. METODOLOGIA ---------- 31
3.2. RISULTATI DELL'ANALISI ---------- 35
3.3. SINTESI DELLE CRITICITÀ RILEVATE ---------- 47
3.4. CONSIDERAZIONI CONCLUSIVE ED ACTION PLAN ---------- 49
3.5. DOCUMENTI DI RIFERIMENTO ---------- 49

4. LA VIDEOSORVEGLIANZA ---------- 51

4.1. SISTEMI DI VIDEOSORVEGLIANZA DI D'AMICO SOCIETÀ DI NAVIGAZIONE S.P.A. ---------- 51
4.2. SISTEMI DI VIDEOSORVEGLIANZA DI D'AMICO SHIPPING ITALIA S.P.A. ---------- 53

1. PREMESSE

1.1. CONTESTO DI RIFERIMENTO: NORMATIVA E ASSUMPTIONS

Al fine di adempiere alle disposizioni del Regolamento Europeo n. 679/2016, di seguito per brevità "il Regolamento", d'Amico Società di Navigazione, di seguito per brevità "DSN", in qualità di Holding del gruppo imprenditoriale d'Amico, di seguito per brevità "gruppo d'Amico", ha predisposto il presente Registro delle attività di trattamento effettuate da DSN e dalla società collegate e controllate, con relativa descrizione delle misure di sicurezza.

La scelta di adottare un unico Registro delle attività di trattamento deriva dall'assetto societario e organizzativo del gruppo d'Amico, che prevede:

- la centralizzazione delle attività Corporate verso le controllate in capo alla Holding DSN, con particolare riferimento ai seguenti ambiti: ICT, HR, Legal & Insurance, HQSE e Finance;
- il medesimo settore economico per DSN e società collegate e/o controllate;
- le medesime categorie di interessati e relative finalità del trattamento per tutte le società del gruppo.

In virtù di tale assetto, DSN ha optato per la nomina di un unico DPO a livello di gruppo, prevedendo delle figure di raccordo a livello locale, denominate Coordinatori privacy, al fine di monitorare la corretta applicazione del sistema organizzativo privacy definito a livello di gruppo all'interno delle Norme Vincolanti d'Impresa (Binding Corporate Rules).

Gli assunti adottati per la realizzazione del presente Registro rispettano i principi di liceità, trasparenza e correttezza contenuti nel Regolamento e i principi rappresentati dalla Cultura organizzativa propria del gruppo d'Amico, che si fondano sull'onestà e sulla fiducia nelle risorse umane. Alla luce di ciò le misure di sicurezza tecniche e organizzative pianificate rispecchiano detti principi.

Si specifica, infine, che il presente documento è stato redatto da DSN in riferimento alle seguenti normative in ambito "privacy":

- art. 30 del Regolamento Europeo n. 679/2016 (di seguito "Regolamento") del 27 aprile 2016;
- Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 recante "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*" (di seguito "Provvedimento relativo agli Amministratori di Sistema");
- Provvedimento del Garante per la protezione dei dati personali dell'8 aprile 2010 in materia di videosorveglianza.

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

1.2. PRINCIPALI DEFINIZIONI

Di seguito si riportano alcune delle principali definizioni introdotte dal Regolamento.

Si definisce «**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.

Si definisce «**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.

Si definisce «**limitazione di trattamento**»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro.

Si definisce «**profilazione**»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.

Si definisce «**pseudonimizzazione**»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

Si definisce «**archivio**»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico.

Si definisce «**titolare del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

Si definisce «responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

Si definisce «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati 4.5.2016 L 119/33 Gazzetta ufficiale dell'Unione europea IT membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento.

Si definisce «terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile.

Si definisce «consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

Si definisce «violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Si definisce «dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.

Si definisce «dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.

Si definisce «dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.

Si definisce «stabilimento principale»: a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale; b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del

trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento.

Si definisce «**rappresentante**»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento.

Si definisce «**impresa**»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica.

Si definisce «**gruppo imprenditoriale**»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate.

Si definisce «**norme vincolanti d'impresa**»: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune.

Si definisce «**autorità di controllo**»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51; 4.5.2016 L 119/34 Gazzetta ufficiale dell'Unione europea IT.

Si definisce «**autorità di controllo interessata**»: un'autorità di controllo interessata dal trattamento di dati personali in quanto: a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo; b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure c) un reclamo è stato proposto a tale autorità di controllo.

Si definisce «**trattamento transfrontaliero**»: a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro.

Si definisce «**obiezione pertinente e motivata**»: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà

fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione.

Si definisce «**servizio della società dell'informazione**»: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio (1).

Si definisce «**organizzazione internazionale**»: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

Si definisce "**dato sensibile**": qualsiasi informazione per la quale la legge prevede una disciplina e una tutela particolari: si tratta dei dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Si definisce "**interessato**": la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.

Si definisce "**amministratore di sistema**": la figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali.

1.3. OBIETTIVI DEL DOCUMENTO

Obiettivo del presente documento è di fornire visibilità in merito alle attività svolte da DSN e società collegate e controllate, relativamente al trattamento dei dati personali degli Interessati, al fine di definire, a titolo esemplificativo e non esaustivo:

- i dati di contatto del Titolare del trattamento e del DPO;
- le categorie di interessati dei quali si detengono i dati e relative finalità di trattamento;
- le categorie di destinatari a cui i dati personali sono o potranno essere comunicati, compresi i destinatari di paesi terzi e/o organizzazioni internazionali;
- l'organizzazione dei compiti e delle responsabilità nell'ambito delle Funzioni preposte al trattamento dei dati;
- l'organigramma privacy;
- le misure di sicurezza tecniche e organizzative adottate in riferimento alle risorse hardware e software utilizzate al fine di garantire un livello di sicurezza adeguato al rischio, quali:
  - 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.

1.4. STRUTTURA DEL DOCUMENTO

Il presente documento si compone di n. 4 (quattro) sezioni.

Nel primo capitolo sono inserite le premesse al presente documento.

Nel secondo capitolo è descritto il Modello Organizzativo adottato da DSN e società collegate e controllate per la gestione degli adempimenti privacy. In tale capitolo sono, pertanto, individuati i seguenti ruoli e responsabilità: Titolare del trattamento, DPO, Responsabili del Trattamento, Classi di incaricati ed Amministratori di sistema. All'interno del capitolo vengono descritte inoltre le categorie di interessati, il tipo di dati trattati e le caratteristiche dei trattamenti effettuati riferiti a DSN e società collegate e controllate ed individuate a seguito dell'assessment effettuato nel corso del 2016 e 2017 a livello di gruppo.

Nel terzo capitolo è riportata l'analisi dei rischi effettuata da DSN a livello Corporate per la Holding e e società collegate e controllate.

Nel quarto capitolo è riportata la parte relativa al sistema di videosorveglianza in essere presso DSN e presso la controllata d'Amico Shipping Italia S.p.A., per brevità di seguito "DSI".

1.5. CONSERVAZIONE DEL DOCUMENTO

Il presente documento è conservato presso la sede operativa di DSN, sita in Roma, Corso d'Italia n. 35b, che ha individuato quale funzione responsabile della conservazione e distribuzione del documento il DPO, i cui dati sono riportati al paragrafo 2.2. "*Responsabile della Protezione dei dati*" del presente documento.

1.6. AMBITO DI DISTRIBUZIONE INTERNA DOCUMENTO

Il presente documento viene pubblicato all'interno della Intranet aziendale in lingua italiana ed inglese e viene tenuto a disposizione degli Interessati e/o delle Autorità di Controllo a cura del DPO e dei Coordinatori privacy in ciascuna sede del gruppo d'Amico.

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

1.7. AGGIORNAMENTO DEL DOCUMENTO

Il presente documento viene aggiornato con cadenza annuale, in occasione della revisione ed aggiornamento del sistema organizzativo privacy del gruppo d'Amico nel suo complesso, fermo restando che le eventuali modifiche ed integrazioni di carattere organizzativo che dovessero intervenire in corso d'anno saranno, comunque, oggetto di adeguamento *in itinere* della documentazione specifica (ad es. a titolo esemplificativo lettere di nomina di Responsabili esterni).

1.8. RESPONSABILE DELL'AGGIORNAMENTO DEL DOCUMENTO

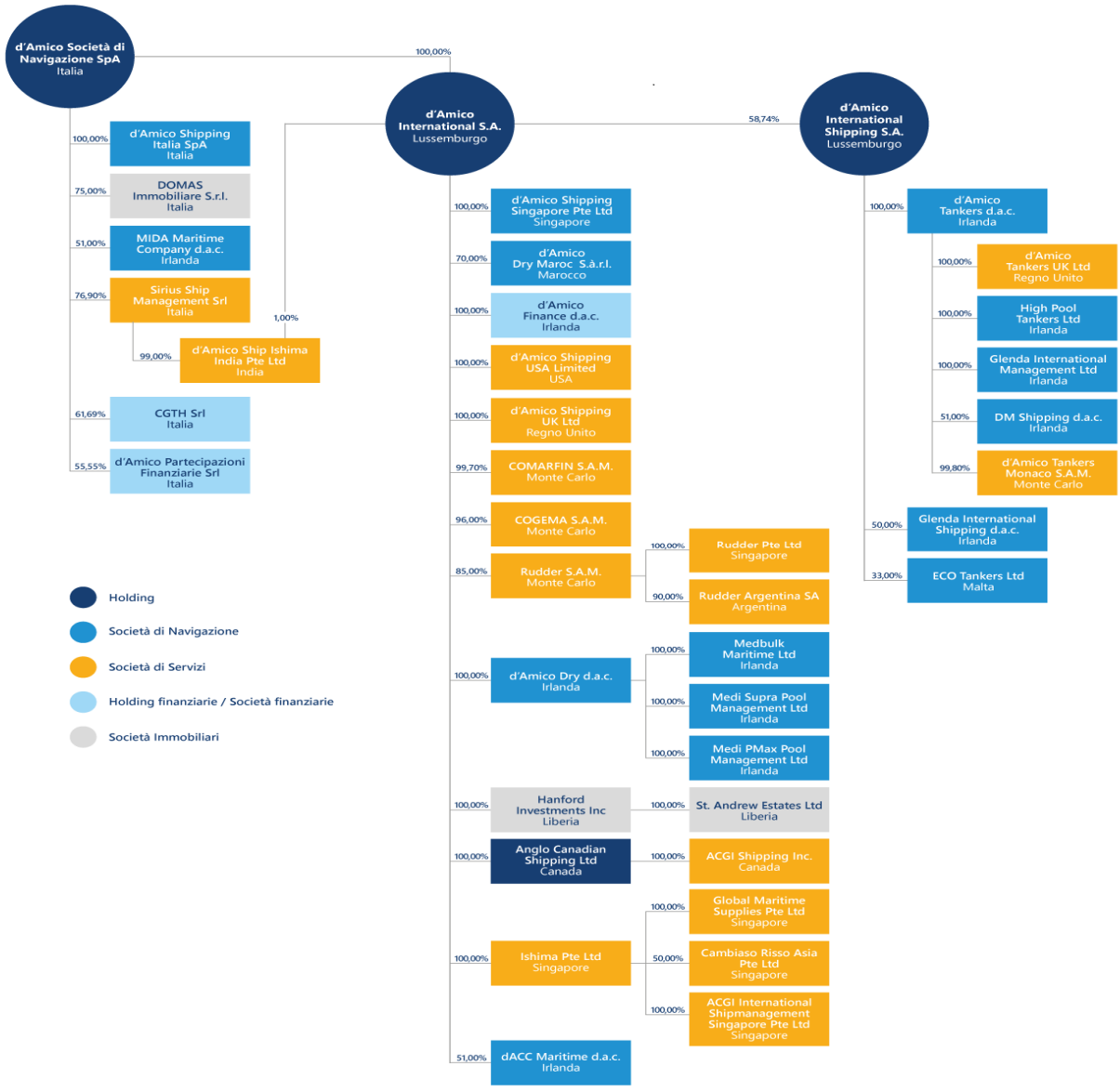
La responsabilità dell'aggiornamento del presente documento viene affidata al DPO.

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

2. IL MODELLO PRIVACY DEL GRUPPO D'AMICO

2.1. LA STRUTTURA DEL GRUPPO D'AMICO

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



Il modello organizzativo privacy di DSN e società collegate e controllate, in linea con quanto previsto dal Regolamento, prevede la Titolarità del trattamento in capo alle singole società a livello locale, fermo restando il ruolo di coordinamento e monitoraggio della corretta attuazione del sistema privacy a livello

di gruppo da parte di DSN, attraverso la figura del Data Protection Officer di gruppo e dei Coordinatori privacy a livello locale.

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[1].	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

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

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
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

2.2. 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 società collegate e/o controllate trattano dati personali, che si riportano di seguito:

- Personale di Terra subordinato e parasubordinato e personale di bordo[2]

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

- Candidati
- Clienti
- Fornitori[3]
- 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 società collegate e 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 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 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.

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

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[4], 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 società collegate e/o 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

[4].*Cfr. Considerando n. 37 del Regolamento.*

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.

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

N.	Società	Paese	Tipologia di società
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

2.2.1. TEMPO DI GESTIONE E CONSERVAZIONE DEI DATI

I criteri utilizzati per determinare il periodo di conservazione applicabile sono: le informazioni personali sono conservate per il tempo (i) necessario al relativo scopo, (ii) necessario all'espletamento del rapporto contrattuale/commerciale in essere, (iii) accettato dall''interessato e/o (iv) richiesto dalle leggi applicabili in materia.

I dati saranno conservati comunque fino al termine di prescrizione dei diritti derivanti dalle obbligazioni assunte.

Per la gestione e conservazione delle immagini relative al sistema di videosorveglianza si rimanda al Capitolo 4 "*Videosorveglianza*" del presente documento.

2.2.2. CANCELLAZIONE DEI DATI

DSN e società collegate e controllate procedono tempestivamente alla cancellazione dei dati riferiti alle categorie di Interessati riportati nel presente paragrafo nei casi previsti dall'articolo 17 del Regolamento.

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

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.

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

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 collegate e/o controllate 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.

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

Candidati

Categoria di dati	Finalità del trattamento	Base giuridica 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	- 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)	Database raccolta cv sito Internet Sharepoint[5] 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 collegate e/o controllate anche extra UE
Società Esterne	n.a.

[5] 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.

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

Clienti

Categoria di dati	Finalità del trattamento	Base giuridica del trattamento	Repository	
			Elettronico	Cartaceo
Dati personali comuni (dati anagrafici, istruzione e cultura ecc.) Dati volti a rilevare il rischio di solvibilità economica e di comportamenti illeciti o fraudolenti Dati Amministrativo-Contabili	*Finalità amministrativo-contabili*: ▪ Adempimento di obblighi fiscali o contabili. ▪ Gestione della clientela (amministrazione della clientela; amministrazione di contratti, ordini, spedizioni e fatture; controllo dell'affidabilità e solvibilità). ▪ Gestione del contenzioso (inadempimenti contrattuali, diffide, transazioni, recupero crediti, arbitrati, controversie giudiziarie). ▪ Servizi di controllo interno (della sicurezza, della produttività, della qualità dei servizi, dell'integrità del patrimonio). ▪ Pianificazione e controllo dei dati economici e finanziari. *Finalità connesse al settore bancario, creditizio e assicurativo*: ▪ Gestione contabile o tesoreria.	- Il trattamento è necessario all'esecuzione di un contratto (rif. art. 6, lettera b. del Regolamento)	- ERP Shipnet - ERP IMOS - Nordic IT - Virtustream - Zantaz - Tagetik - DUALOG - Exchange Server	- Archivio cartaceo presso la funzione Accounting 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 collegate e/o controllate
Società Esterne	n.a.

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

Fornitori[6]

Categoria di dati	Finalità del trattamento	Base giuridica del trattamento	Repository	
			Elettronico	Cartaceo
Dati personali comuni (dati anagrafici, istruzione e cultura ecc.) Dati Amministrativo-Contabili	*Finalità amministrativo-contabili*: ▪ Adempimento di obblighi fiscali o contabili. ▪ Gestione dei fornitori (amministrazione dei fornitori; amministrazione di contratti, ordini, arrivi e fatture; selezioni in rapporto alle necessità dell'impresa, controllo dell'affidabilità). ▪ Pianificazione e controllo dei dati economici e finanziari. *Finalità connesse al settore bancario, creditizio e assicurativo*: ▪ Gestione contabile o tesoreria.	- Il trattamento è necessario all'esecuzione di un contratto (rif. art. 6, lettera b. del Regolamento)	- ERP Shipnet - ERP IMOS - Nordic IT - Virtustream - Zantaz - Tagetik - DUALOG - Exchange Server.	- Archivio cartaceo presso la funzione Purchasing 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., d'Amico Shipping Singapore Pte Ltd, ISHIMA Pte Ltd
Società Esterne	n.a.

[6] Comprendono anche i cantieri a cui vengono affidati i lavori per la costruzione delle nuove navi (Vietnam e Giappone).

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

Visitatori

Categoria di dati	Finalità del trattamento	Base giuridica del trattamento	Repository	
			Elettronico	Cartaceo
Dati personali comuni (dati anagrafici)	*Finalità amministrativo-contabili*: ▪ Gestione degli accessi. ▪ Tutela della sicurezza.	- L'interessato ha espresso il consenso al trattamento dei propri dati personali per le specifiche finalità (rif. art. 6, lettera a. del Regolamento).	- n.a.	- Registro cartaceo degli ingressi.

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 collegate e/o controllate
Società Esterne	n.a.

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

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

Categoria di dati	Finalità del trattamento	Base giuridica del trattamento	Repository	
			Elettronico	Cartaceo
Dati personali comuni (dati anagrafici, istruzione e cultura, ecc) Dati Amministrativo-Contabili	*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.	- 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)	- Multipartner - Nordic IT - IT2 - Zantaz - Tagetik - DUALOG - Exchange Server	- Archivio cartaceo presso il Legal & Insurance 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 collegate e/o controllate anche extra UE
Società Esterne	Società di selezione del personale in qualità di Responsabili esterni del trattamento dei dati

2.3. RUOLI E RESPONSABILITA' IN AMBITO PRIVACY

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

2.3.1. TITOLARE DEL TRATTAMENTO

In qualità di Titolare del trattamento, DSN e le società collegate e/o controllate 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).

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

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

In ottemperanza all' art. 37 del Regolamento, DSN ha designato quale Responsabile della Protezione dei dati a livello di gruppo, di seguito DPO, in staff al Titolare del Trattamento di DSN.

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'HR Department.

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 rimosso o 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 a DSN e alle società collegate e/o controllate 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 da DSN per ogni società del gruppo d'Amico;
b) informare e fornire consulenza a DSN e alle società collegate e/o controllate 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 dei Titolari 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.

2.3.3. COORDINATORE PRIVACY (ART.37 COMMA 2)

In ottemperanza al comma 2 dell'art. 37 del Regolamento, DSN, al fine di agevolare il coordinamento e la gestione delle azioni volte al rispetto del sopracitato Regolamento, ha nominato, per ogni country del gruppo a livello internazionale, un Coordinatore Privacy.

Tale figura è coordinata dal DPO.

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 l'ufficio HR.

2.3.4. 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).

Il gruppo d'Amico ha distinto la figura del Responsabile tra:

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

2.3.4.1. RESPONSABILI INTERNI PRIVACY

DSN e società collegate e/o controllate, in qualità di Titolari del Trattamento, hanno nominato in qualità di Responsabili interni Privacy i Responsabili delle Funzioni Organizzative, che nell'ambito delle proprie

attribuzioni, trattano manualmente o con strumenti elettronici, dati personali di cui il gruppo d'Amico è Titolare.

Tali 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 la struttura del DPO di gruppo.

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

2.3.4.2. RESPONSABILI ESTERNI PRIVACY

DSN e società collegate e/o controllate, in qualità di Titolari del Trattamento, hanno nominato in qualità di Responsabili Esterni Privacy le società e i professionisti che forniscono servizi alle singole società del gruppo d'Amico, che nell'ambito dell'incarico ricevuto dalle società del gruppo d'Amico, trattano manualmente o con strumenti elettronici, dati personali di cui il gruppo d'Amico è Titolare.

DSN ha delineato due diverse tipologie di Responsabile esterno, differenziando tale ruolo in:

a) Responsabile esterno infra-gruppo;

b) Responsabile esterno al di fuori del gruppo.

Tali nomine sono formalizzate attraverso una lettera di nomina sulla base dei trattamenti effettuati da ciascun Responsabile esterno che ne disciplina i compiti; copia delle lettere di nomina controfirmate dal Responsabile sono archiviate sono archiviate presso la struttura del DPO di gruppo.

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

2.3.5. CLASSI DI INCARICATI

DSN e società collegate e/o controllate, in qualità di 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 società collegate e/o controllate sono Titolari.

Tali designazioni sono formalizzate attraverso apposita lettera che ne disciplina i compiti; le copie delle lettere di designazione controfirmate per presa visione dagli incaricati sono archiviate sono archiviate presso la struttura del DPO di gruppo.

2.3.6. AMMINISTRATORI DI SISTEMA (ADS)

DSN e società collegate e/o controllate, in qualità di 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*"..

3. L'ANALISI DEI RISCHI (art.32)

Nel presente capitolo è riportata l'analisi dei rischi effettuata tra la fine del 2016 e il primo trimestre 2017 da DSN per tutte le società del gruppo d'Amico e finalizzata a:

- rilevare le misure di sicurezza tecniche ed organizzative in essere all'interno del gruppo d'Amico in riferimento alla sicurezza dei dati personali;
- valutarne la relativa adeguatezza;
- definire le eventuali misure da implementare per garantire il rispetto della normativa in tema di protezione dei dati personali.

Gli elementi presi in considerazione per l'analisi e valutazione dei rischi, in conformità a quanto previsto dal Regolamento, sono riportati di seguito,

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

A completamento dello scenario, si specifica che l'ambito dell'analisi dei rischi è da intendersi riferito esclusivamente ai dati personali e ai relativi trattamenti che gli Incaricati svolgono su di essi nell'ambito delle attività svolte all'interno del gruppo d'Amico.

Nei paragrafi successivi viene presentata la metodologia di riferimento utilizzata nonché i risultati dell'analisi e la sintesi delle criticità rilevate.

3.1. METODOLOGIA

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.

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

3.1.1. 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.

3.1.2. 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.

3.1.3. 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.

3.1.4. 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.).

3.1.5. 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.

3.1.6. 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

3.1.7. 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.

3.1.8. 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

3.1.9. 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.

3.2. RISULTATI DELL'ANALISI

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

3.2.1. 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.

3.2.2. 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 dal fornitore BT, 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:

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

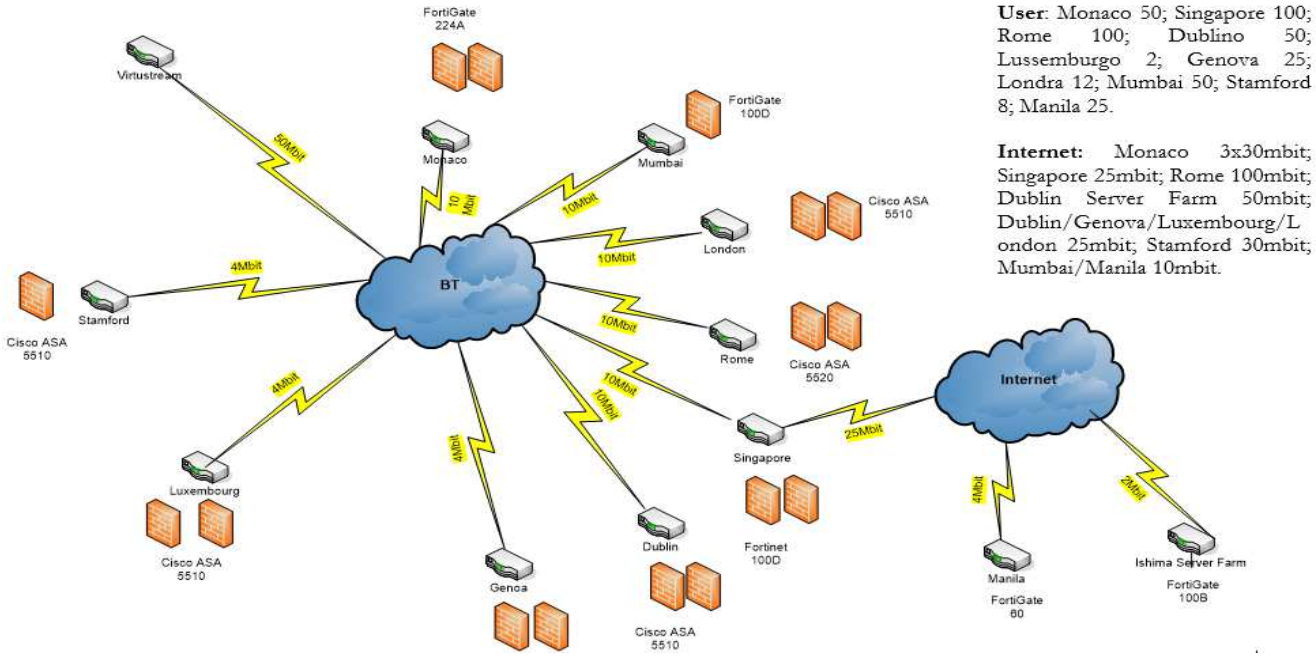


Figura 1 – Articolazione infrastruttura tecnologica d'Amico Group

A completamento della sotto-fase, nella tabella seguente, sono riportati gli applicativi e le relative basi dati presenti in DSN e società collegate e/o controllate, che ricadono nel campo di applicazione del Regolamento.

Applicativi	Descrizione sistema	Banche Dati Gestite
SHIPNET	ERP	Clienti Fornitori
INTERNATIONAL MARITIME OPERATION SYSTEM (IMOS)	ERP per la gestione del Chartering e Operations	Clienti Fornitori
MARK V	Sistema accessorio di gestione della posta elettronica	ALL
DUALOG	Piattaforma digitale per la gestione della posta elettronica di bordo	ALL
MIMECAST	Sistema di mail continuity (back up di posta temporaneo)	ALL
IT2	Il Sistema è gestito da: - *Finance Dept.* per la gestione della tesoreria di Gruppo - *ICT Dept.* per la gestione delle credenziali.	Personale di terra (Dipendenti) Clienti Fornitori
SHAREPOINT	Piattaforma software di Content Management System (CMS) per la gestione del portale aziendale	Personale di terra

ZANTAZ	Sistema di archiviazione posta	Personale di terra, clienti, fornitori e Componenti degli organi
WATCHKEEPER	Sistema per il monitoraggio del personale di bordo (ad esempio ore lavorative da parte del personale di bordo)	Personale di Bordo
TNSJ TRAVEL	Applicazione per la gestione delle trasferte	Personale di terra
WEB SITE - GESTIONE CANDIDATURE	Sistema di acquisizione candidature	Candidati e colloquiandi
Exchange Server	Sistema di gestione della posta elettronica	ALL

3.2.3. 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 archivi cartacei;
- Sicurezza Data Center di gruppo;
- Sicurezza logica degli accessi;
- Sicurezza dei dati;
- Sicurezza della rete;
- Sicurezza degli applicativi;
- Sicurezza logica;
- Sicurezza workstation.

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

3.2.4. 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	Adeguato	Basso

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

Contesto	Evento	Fattore di Rischio	Impatto	Probabilità	Rischio Inerente	Misura di protezione in essere	Valutazione dei controlli	Rischio Residuo
						- PIM		
Comportamento degli operatori	Furto di strumenti contenenti dati	- Omessa custodia	B	B	B	- Codice Etico - PIM	Adeguato	Basso
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	Parziale	Medio

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

Contesto	Evento	Fattore di Rischio	Impatto	Probabilità	Rischio Inerente	Misura di protezione in essere	Valutazione dei controlli	Rischio Residuo
						- Codice Etico		
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) - Violazione sistemi antiintrusione	M	B	B	- Badge (ove applicabile) - Codice Etico - Porte chiuse a chiave (ove applicabile)	Adeguato	Basso
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

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

Contesto	Evento	Fattore di Rischio	Impatto	Probabilità	Rischio Inerente	Misura di protezione in essere	Valutazione dei controlli	Rischio Residuo
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 tipologie di utenze e per tutti i sistemi e server in linea con la posizione ricoperta - Assenza di una politica di controllo degli accessi	M	B	B	- ITG-09 User Accounts - Monitoraggio dei tentativi di accesso falliti	Adeguato	Basso

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

Contesto	Evento	Fattore di Rischio	Impatto	Probabilità	Rischio Inerente	Misura di protezione in essere	Valutazione dei controlli	Rischio Residuo
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

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

Contesto	Evento	Fattore di Rischio	Impatto	Probabilità	Rischio Inerente	Misura di protezione in essere	Valutazione dei controlli	Rischio Residuo
Sicurezza della rete	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 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

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

Contesto	Evento	Fattore di Rischio	Impatto	Probabilità	Rischio Inerente	Misura di protezione in essere	Valutazione dei controlli	Rischio Residuo
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
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

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

Contesto	Evento	Fattore di Rischio	Impatto	Probabilità	Rischio Inerente	Misura di protezione in essere	Valutazione dei controlli	Rischio Residuo
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

3.3. SINTESI DELLE CRITICITÀ RILEVATE

Nella Tabella seguente sono riepilogati, per ciascuna tipologia di rischio residuo valutato come "MEDIO", le azioni da intraprendere per superare le relative criticità.

Contesto	Evento	Fattore di Rischio	Rischio Inerente	Misura di protezione in essere	Valutazione dei controlli	Rischio residuo	Risposta al rischio residuo			
							Accettato	Ridotto	Evitato	Trasferito
Backup dei dati	Distruzione e perdita dati	- Indisponibilità dei dati	M	- SLA di Contratto	Parziale	Medio		Revisione della procedura di Back-up in essere Disaster recovery Revisione BIA Cloud del file system		
Gestione incident	Malfunzionamento, indisponibilità delle applicazioni	- Inadeguato monitoraggio	M	- ITG-07 ERP Trouble Ticketing	Parziale	Medio		Monitoraggio dei log di incident Database degli incident WorkAround		
Sicurezza logica	Azione di virus informatici o di programmi suscettibili di provocare danno	- Mancato aggiornamento dei software di contrasto	A	- Antivirus centralizzato ed aggiornamenti automatici non disattivabili dagli utenti - Penetration test annuale	Adeguato	Medio	X			

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

Contesto	Evento	Fattore di Rischio	Rischio Inerente	Misura di protezione in essere	Valutazione dei controlli	Rischio residuo	Risposta al rischio residuo			
							Accettato	Ridotto	Evitato	Trasferito
				- Monitoraggio del comportamento verso Internet - Monitoraggio dell'attività interna di rete						

3.4. CONSIDERAZIONI CONCLUSIVE ED ACTION PLAN

Dall'analisi effettuata emerge un quadro complessivo di sostanziale adeguatezza del sistema dei controlli in essere all'interno di DSN e società collegate e/o controllate, 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.

3.5. 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.

4. LA VIDEOSORVEGLIANZA

DSN e la società controllata DSI, in relazione alle attività di business e alle esigenze di tutela della sicurezza e del patrimonio aziendale, hanno provveduto a richiedere alle Autorità competenti le autorizzazioni necessarie all'installazione di impianti di videosorveglianza all'interno delle seguenti sedi operative:

- Genova, Via dei Marini n. 53 – Torre Shipping Scala A
- Roma, Corso d'Italia 35b

Si riportano di seguito gli estremi dei Provvedimenti autorizzativi rilasciati dalle Autorità competenti e il dettaglio dei sistemi di videosorveglianza installati.

4.1. SISTEMI DI VIDEOSORVEGLIANZA DI D'AMICO SOCIETÀ DI NAVIGAZIONE S.P.A.

Genova, Via dei Marini n. 53 – Torre Shipping Scala A

Con Decreto n. 154 del 03/12/2012, DSN ha ricevuto dal Ministero del Lavoro e delle Politiche Sociali - Direzione Territoriale del Lavoro di Genova, l'autorizzazione all'installazione di un sistema di videosorveglianza presso la sede operativa della società, sita in Via dei Marini n. 53 – Torre Shipping Scala A, a Genova.

Il sistema di videosorveglianza si compone di n. 2 telecamere fisse interne e da n. 1 unità di videoregistrazione.

Roma, Corso d'Italia 35b

Con Provvedimento Prot. n. 85023 del 13/09/2013, DSN ha ricevuto dal Ministero del Lavoro e delle Politiche Sociali - Direzione Territoriale del Lavoro di Roma, l'autorizzazione all'installazione di un sistema di videosorveglianza presso la sede operativa della società, sita in Corso d'Italia 35b a Roma.

Il sistema di videosorveglianza si compone di n. 21 telecamere fisse interne, n. 3 telecamere fisse esterne, n. 1 sistema di videoregistrazione e n. 3 monitor dislocati come segue:

n. 21 telecamere, distribuite nelle seguenti aree:

- n. 2 telecamere al piano seminterrato;

- n. 5 telecamere al piano terra;

- n. 7 telecamere al piano primo;

- n. 3 telecamere al piano secondo;

- n. 6 telecamere al piano terzo;

n. 3 telecamere, distribuite nelle seguenti aree:

- n. 2 telecamere nell'area parcheggio;

- n. 1 telecamera nell'androne del palazzo;

n. 1 sistema di videoregistrazione installato al piano secondo

n. 3 monitor dislocati nelle seguenti aree:

- n. 1 monitor al piano terra;

- n. 1 monitor al piano primo;

- n. 1 monitor al piano terzo.

A fronte dei Provvedimenti autorizzativi ricevuti, d'Amico Società di Navigazione S.p.A. ha provveduto a formalizzare le relative nomine dei Responsabili per detti sistemi di sorveglianza e a designare le relative classi di incaricati.

Si riportano di seguito i nominativi dei Responsabili nominati e delle relative finalità dei trattamenti.

Responsabile Interno	Strutture ove si trova/trovano la/e telecamera/e	Categoria di Interessati	Finalità di trattamento -
Francesco Rotundo	Area esterna: parcheggio e androne Area interna: piano seminterrato, piano terra, piano primo, piano secondo e piano terzo	Tutte le categorie di interessati che accedono alle sedi di Genova e Roma, compreso il personale dipendente	Finalità di prevenzione di eventuali furti, danneggiamenti o atti di vandalismo e di prevenzione incendi nonché per la sicurezza dei lavoratori.

Per maggiori dettagli si rimanda all'apposita informativa, disponibile presso la sede di d'Amico Società di Navigazione S.p.A..

4.2. SISTEMI DI VIDEOSORVEGLIANZA DI D'AMICO SHIPPING ITALIA S.P.A.

Genova, Via dei Marini n. 53 – Torre Shipping Scala A

Con Decreto n. 157 del 17/12/2012, d'Amico Shipping Italia S.p.A. ha ricevuto dal Ministero del Lavoro e delle Politiche Sociali - Direzione Territoriale del Lavoro di Genova, l'autorizzazione all'installazione di un sistema di videosorveglianza presso la sede operativa della società, sita in Via dei Marini n. 53 – Torre Shipping Scala A a Genova.

Il sistema di videosorveglianza si compone di n. 2 telecamere fisse interne e da n. 1 unità di videoregistrazione.

Roma, Corso d'Italia 35b

Con Provvedimento Prot. n. 95430 del 08/10/2013, DSI ha ricevuto dal Ministero del Lavoro e delle Politiche Sociali - Direzione Territoriale del Lavoro di Roma, l'autorizzazione all'installazione di un sistema di videosorveglianza presso la sede operativa della società, sita in Corso d'Italia 35b a Roma.

Il sistema di videosorveglianza si compone di n. 21 telecamere fisse interne, n. 3 telecamere fisse esterne, n. 1 sistema di videoregistrazione e n. 3 monitor dislocati come segue:

n. 21 telecamere, distribuite nelle seguenti aree:

- n. 2 telecamere al piano seminterrato;

- n. 5 telecamere al piano terra;

- n. 7 telecamere al piano primo;

- n. 3 telecamere al piano secondo;

- n. 6 telecamere al piano terzo;

n. 3 telecamere, distribuite nelle seguenti aree:

- n. 2 telecamere nell'area parcheggio;

- n. 1 telecamera nell'androne del palazzo;

n. 1 sistema di videoregistrazione installato al piano secondo

n. 3 monitor dislocati nelle seguenti aree:

- n. 1 monitor al piano terra;

- n. 1 monitor al piano primo;

- n. 1 monitor al piano terzo.

A fronte del Provvedimento autorizzativo ricevuto, d'Amico Shipping Italia S.p.A. ha provveduto a formalizzare le relative nomine dei Responsabili per detti sistemi di sorveglianza e a designare le relative classi di incaricati.

Si riportano di seguito i nominativi dei Responsabili nominati e delle relative finalità dei trattamenti.

Responsabile Interno	Strutture ove si trova/trovano la/e telecamera/e	Categoria di Interessati	Finalità di trattamento -
Francesco Rotundo	Area esterna: parcheggio e androne Area interna: piano seminterrato, piano terra, piano primo, piano secondo e piano terzo	Tutte le categorie di interessati che accedono alle sedi di Genova e Roma, compreso il personale dipendente	Finalità di prevenzione di eventuali furti, danneggiamenti o atti di vandalismo e di prevenzione incendi nonché per la sicurezza dei lavoratori.
Paola Cappabianca	Area esterna: parcheggio e androne Area interna: piano seminterrato, piano terra, piano primo, piano secondo e piano terzo	Tutte le categorie di interessati che accedono alle sedi di Genova e Roma, compreso il personale dipendente	Finalità di prevenzione di eventuali furti, danneggiamenti o atti di vandalismo e di prevenzione incendi nonché per la sicurezza dei lavoratori.

Per maggiori dettagli si rimanda all'apposita informativa, disponibile presso la sede di d'Amico Shipping Italia S.p.A..