RECORDS OF PROCESSING ACTIVITIES

D'AMICO GROUP

Issued	*Approved*
Data Protection Officer	*HR Department*

Distribution

All Data Processors and operators

References: : EU Regulation n. 2016/679 of April 27, 2016

Index

References: : EU Regulation n. 2016/679 of April 27, 2016

1. PREMISE

1.1. CONTEXT: LEGISLATION AND ASSUMPTIONS

In order to comply with the provisions of the European Regulation no. 679/2016, hereinafter referred to as "the Regulation", d'Amico Società di Navigazione, hereinafter referred to as "DSN" for the sake of brevity, as a holding of the d'Amico business group, hereinafter referred to as "d'Amico group", has prepared this Register of processing activities carried out by DSN and its group undertakings, with a description of the security measures adopted.

The decision to adopt a single Record of the processing activities derives from the corporate and organizational structure of d'Amico group, which includes::

- the centralization of Corporate activities towards the group undertakings of the Holding DSN, with particular reference to the following areas: ICT, HR, Legal & Insurance, HQSE and Finance;
- the same economic sector for DSN and its group undertakings;
- the same categories of data subjects and related purposes of processing for all group's companies.

By virtue of this structure, DSN opted for the appointment of a single DPO at group level, envisaging local connection figures, called Privacy Coordinators, in order to monitor the correct application of the organizational privacy system defined at group level within the binding corporate rules (Binding Corporate Rules).

The assumptions adopted for the realization of the present Record respect the principles of lawfulness, transparency and fairness contained in the Regulations and the principles represented by the organizational culture of the d'Amico group, which are based on honesty and trust in human resources. In light of this, the planned technical and organizational security measures reflect these principles.

Finally, it is specified that this document was drafted by DSN with reference to the following "privacy" regulations:

- art. 30 of EU Regulation no. 2016/679 (hereinafter "Regulation") of April 27, 2016;
- Decision dated 27 November 2008 of the Italian Data Protection Authority *"Measures and arrangements applying to the controllers of processing operations performed with the help of electronic tools in view of committing the task of system administrator* (hereinafter "Decision on System Administrator");
- Decision of the Italian DPA on Video-surveillance of April 8, 2010.

References: : EU Regulation n. 2016/679 of April 27, 2016

1.2. MAIN DEFINITIONS

The following are some of the main definitions introduced by the Regulation.

Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Restriction of processing means the marking of stored personal data with the aim of limiting their processing in the future.

Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Filing system means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Recipient means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the 4.5.2016 L 119/33 Official Journal of the European Union EN framework of a particular inquiry

in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

Third party means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Genetic data means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

Biometric data means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

Data concerning health means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

Main establishment means: a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment; b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation.

Representative means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation.

Enterprise means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity.

Group of undertakings means a controlling undertaking and its controlled undertakings.

Binding corporate rules means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.

Supervisory authority means an independent public authority which is established by a Member State pursuant to Article 51.

Supervisory authority concerned means a supervisory authority which is concerned by the processing of personal data because: a) the controller or processor is established on the territory of the Member State of that supervisory authority; b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or c) a complaint has been lodged with that supervisory authority.

Cross-border processing means either: a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

Relevant and reasoned objection means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union.

Information society service means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council.

International organisation means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.

1.3. DOCUMENT OBJECTIVES

The objective of this document is to provide visibility on the activities carried out by DSN and its group undertakings, with regard to the processing of personal data of data subjects, in order to define, by way of example and not exhaustively:

- The contact details of Data Controller and DPO;

- the categories of data subjects and the related purposes of the processing;
- the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
- the organization of tasks and responsibilities within the functions involved in data processing;
- the privacy organization chart;
- the technical and organizational security measures adopted with reference to the hardware and software resources used in order to ensure an appropriate level of security to the risk, as:
  - the pseudonymisation and encryption of personal data;
  - the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
  - the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
  - a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

1.4. DOCUMENT STRUCTURE

This document consists of n. 4 (four) chapters.

The first chapter contains the premises for this document.

The second chapter describes the Organizational Model adopted by DSN and its group undertakings for the management of privacy obligations. Therefore, in this chapter the following roles and responsibilities are identified: Data Controller, DPO, Data Processors, Persons in charge of the processing and System Administrators.
The chapter also describes the categories of data subjects, the type of data processed and the characteristics of the performed processing referring to DSN and its group undertakings and identified after the assessment carried out during 2016 and 2017 at group level.

The third chapter shows the risk analysis carried out by DSN at Corporate level for the Holding and its group undertakings.

The fourth chapter reports the part related to the video surveillance system in place at DSN and at its subsidiary d'Amico Shipping Italia S.p.A., hereinafter "DSI".

References: : EU Regulation n. 2016/679 of April 27, 2016

1.5. CONSERVATION OF THE DOCUMENT

This document is kept at the headquarters of DSN, located in Rome, Corso d'Italia n. 35b, which has identified the DPO as responsible for the conservation and distribution of the document, whose data are reported in paragraph 2.2. "Data Protection Officer" of this document.

1.6. INTERNAL DISTRIBUTION OF THE DOCUMENT

This document is published on the company Intranet in Italian and English language and is kept available to the data subjects and / or the supervisory authorities by the DPO and the privacy coordinators in each of d'Amico group offices.

1.7. UPDATES

This document is updated every year, on the occasion of the revision and updating of the d'Amico group's overall organizational privacy system, without prejudice to the fact that any changes and additions of an organizational nature that may occur during the year will, however, be subject to ongoing adaptation of specific documentation (for example, letters of appointment of external data processors).

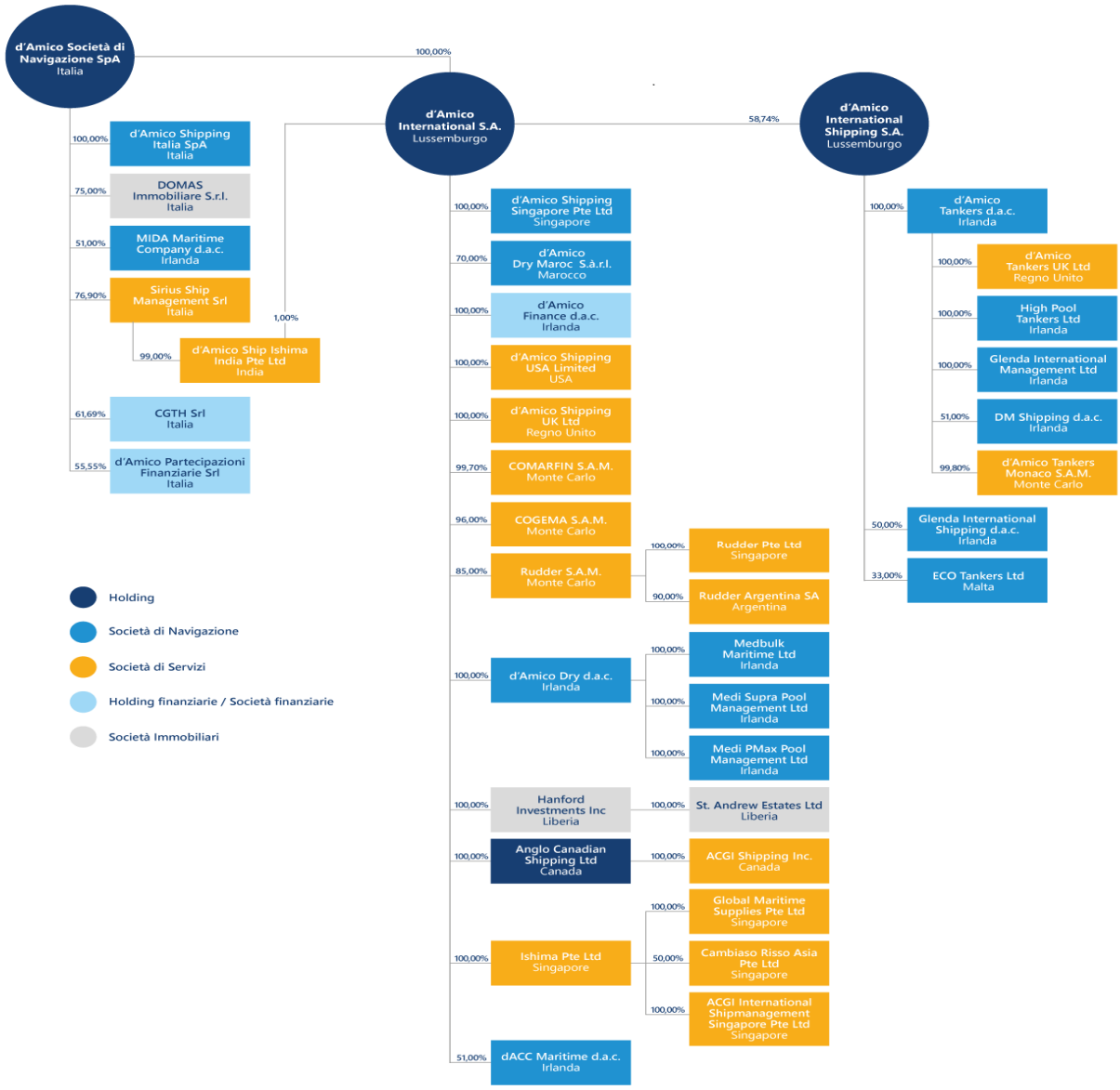
The responsibility for updating this document is entrusted to the DPO.

References: : EU Regulation n. 2016/679 of April 27, 2016

2. THE ORGANIZATIONAL PRIVACY MODEL OF D'AMICO GROUP

2.1. D'AMICO GROUP STRUCTURE

The structure of d'Amico group as of June 30, 2017 is reported below.



The privacy organizational model of DSN and its group undertakings, in line with the provisions of the Regulation, identify the individual companies at local level as Data Controllers, without prejudice to the

role of coordination and monitoring of the correct implementation of the privacy system at group level on behalf of DSN, through the figure of the Group Data Protection Officer and the local privacy coordinators.

In particular, n.41 companies, located in the following countries, compose d'Amico group, as of 30th June 2017:

- Italy
- Luxembourg
- Principality of Monaco
- United Kingdom
- Ireland
- Malta
- USA
- Canada
- Singapore
- India
- Morocco
- Argentina
- Liberia

A list of companies by country and by kind of activity carried out within d'Amico group is reported below:

N.	Company	Country	Type of company
1	d'Amico Società di Navigazione S.p.A.	Italy	Holding
2	d'Amico Shipping Italia S.p.A.	Italy	Shipping company
3	DOMAS Immobiliare S.r.l.	Italy	Real estate company
4	d'Amico Partecipazioni Finanziarie S.r.l.	Italy	Financial company
5	Sirius Ship Management Srl	Italy	Service company
6	CGTH Srl	Italy	Financial company
7	d'Amico International S.A[1].	Luxembourg	Holding
8	d'Amico International Shipping S.A.	Luxembourg	Holding

[1] It controls the 50% of the share of d'Amico International Shipping S.A..

References: : EU Regulation n. 2016/679 of April 27, 2016

9	d'Amico Tankers Monaco S.A.M.	Principality of Monaco	Service company
10	Cogema S.A.M.	Principality of Monaco	Service company
11	Comarfin S.A.M.	Principality of Monaco	Service company
12	Rudder S.A.M.	Principality of Monaco	Service company
13	d'Amico Dry d.a.c.	Ireland	Shipping company
14	MIDA Maritime Company d.a.c.	Ireland	Shipping company
15	Medbulk Maritime Ltd	Ireland	Shipping company
16	Medi Supra Pool Management Ltd	Ireland	Shipping company
17	Medi PMax Pool Management Ltd	Ireland	Shipping company
18	d'Amico Tankers d.a.c.	Ireland	Shipping company
19	d'Amico Finance d.a.c.	Ireland	Financial Company
20	dACC Maritime d.a.c.	Ireland	Shipping company
21	High Pool Tankers Ltd	Ireland	Shipping company
22	Glenda International Shipping Ltd	Ireland	Shipping company
23	DM Shipping Ltd	Ireland	Shipping company
24	Glenda International Management Ltd	Ireland	Shipping company
25	d'Amico Shipping UK Ltd	United Kingdom	Service company
26	d'Amico Tankers UK Ltd	United Kingdom	Service company
27	ECO Tankers Ltd	Malta	Shipping company
28	d'Amico Shipping Singapore Pte Ltd	Singapore	Shipping company
29	ISHIMA Pte Ltd	Singapore	Service company
30	Global Maritime Supplies Pte Ltd	Singapore	Service company
31	ACGI Pte Ltd	Singapore	Service company
32	Cambiaso Risso Asia	Singapore	Service company
33	Rudder Pte Ltd	Singapore	Service company
34	Anglo Canadian Shipping Ltd	Canada	Holding
35	ACGI Shipping Inc	Canada	Service company
36	d'Amico Ship Ishima India Ltd	India	Service company
37	d'Amico Dry Maroc S.a.r.l.	Morocco	Shipping company
38	Rudder Argentina SA	Argentina	Service company
39	d'Amico Shipping USA Limited	USA	Service company
40	Hanford Investments Inc	Liberia	Real estate company
41	St. Andrew Estates Ltd	Liberia	Real estate company

References: : EU Regulation n. 2016/679 of April 27, 2016

2.2. DECLINATION OF D'AMICO GROUP STRUCTURE'S PRIVACY MODEL

In light of the framework outlined above, and with particular reference to the provisions of the Regulations on business groups[2], the privacy model has been implemented on the d'Amico Group structure.

The first step for the declination of the privacy model was to define the perimeter of the companies falling into the model (*in scope and out of scope* with the model).

This activity was carried out using the main criterion of the "dominant influence" exercised by DSN on its controlled undertakings.

The concept of "*dominant influence*" has been borrowed by Recital n.37 of the Regulation 2016/679, reported below:

"A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exert a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented".

By virtue of this definition, a first classification of the companies was carried out, according to the division into "*in scope*" and "*out of scope*" companies with the model.

Following this first classification, we proceeded with the application of a second criterion, relating to the core business of the *out-of-scope* companies, in order to verify whether it was appropriate to include within the model those companies that, even in the absence of one or more of the criteria enunciated by the Regulations, they are configured as "shipping companies".

At the end of this reclassification, we proceeded to the analysis and the weighting of the results through the application of more subjective criteria to manage "specific" situations, such as the presence, within the companies resulting from the reclassification as *out of scope* with the model, of personnel employed by companies *in scope* to the model.

In light of this additional weighting criterion, the definitive perimeter of the companies *in scope and out of scope* with the privacy model has been outlined, the rationals of which consists in the roles and responsibilities of the Holding and the group undertakings.

- Companies *in scope* with the model: these companies are framed within the privacy model as autonomous data controllers within the group.

[2] *Recital n. 37* of the Regulation.

For these companies DSN will exercise the role of direction, monitoring and control in the field of privacy, being able to exercise a dominant influence on the strength of the criteria set out above. This role will be carried out by providing the necessary support in terms of assistance, consulting and a common documental framework.

- Companies *out of scope* with the model: these companies are classified within the model as autonomous data controllers outside the group.

  For these companies DSN will not exercise the role of direction in privacy matters, without prejudice to the control of their work as companies within the d'Amico group and the support on request from the group undertakings.

The list of the companies, as reclassified in the light of the assessment activities, is reported below:

- n. 32 companies of the group, as autonomous data controllers within the model *(in scope* with the model)

N.	Company	Country	Type of company
1	d'Amico Società di Navigazione S.p.A.	Italy	Holding
2	d'Amico Shipping Italia S.p.A.	Italy	Shipping company
3	Sirius Ship Management Srl	Italy	Service company
4	d'Amico International S.A[1].	Luxembourg	Holding
5	Cogema S.A.M.	Principality of Monaco	Service company
6	Comarfin S.A.M.	Principality of Monaco	Service company
7	d'Amico Dry d.a.c.	Ireland	Shipping company
8	Medbulk Maritime Ltd	Ireland	Shipping company
9	Medi PMax Pool Management Ltd	Ireland	Shipping company
10	d'Amico Shipping UK Ltd	United Kingdom	Service company
11	d'Amico Shipping Singapore Pte Ltd	Singapore	Shipping company
12	d'Amico International Shipping S.A.	Luxembourg	Holding
13	d'Amico Tankers Monaco S.A.M.	Principality of Monaco	Service company
14	d'Amico Ship Ishima India Ltd	India	Service company
15	d'Amico Shipping USA Limited	USA	Service company
16	Hanford Investments Inc	Liberia	Real estate company
17	St. Andrew Estates Ltd	Liberia	Real estate company
18	d'Amico Tankers d.a.c.	Ireland	Shipping company
19	dACC Maritime d.a.c.	Ireland	Shipping company
20	High Pool Tankers Ltd	Ireland	Shipping company

References: : EU Regulation n. 2016/679 of April 27, 2016

N.	Company	Country	Type of company
21	Glenda International Shipping Ltd	Ireland	Shipping company
22	DM Shipping Ltd	Ireland	Shipping company
23	Glenda International Management Ltd	Ireland	Shipping company
24	d'Amico Tankers UK Ltd	United Kingdom	Service company
25	MIDA Maritime Company d.a.c.	Ireland	Shipping company
26	d'Amico Dry Maroc S.a.r.l.	Morocco	Shipping company
27	Medi Supra Pool Management Ltd	Ireland	Shipping company
28	ISHIMA Pte Ltd	Singapore	Service company
29	ACGI Pte Ltd	Singapore	Service company
30	Anglo Canadian Shipping Ltd	Canada	Holding
31	ACGI Shipping Inc	Canada	Service company
32	DOMAS Immobiliare S.r.l.	Italy	Real estate company

- n. 9 group's companies, as autonomous data controllers, out of scope with the model

N.	Company	Country	Type of company
1	d'Amico Partecipazioni Finanziarie S.r.l.	Italy	Financial company
2	CGTH Srl	Italy	Financial company
3	ECO Tankers Ltd	Malta	Shipping company
4	Cambiaso Risso Asia Pte Ltd	Singapore	Service company
5	Rudder Argentina SA	Argentina	Service company
6	d'Amico Finance d.a.c.	Ireland	Financial company
7	Rudder S.A.M.	Principality of Monaco	Service company
8	Rudder Pte Ltd	Singapore	Service company
9	Global Maritime Supplies Pte Ltd	Singapore	Service company

2.3. CATEGORIES OF DATA SUBJECTS OF D'AMICO GROUP

During the assessment activities, in addition to define the responsibilities of the companies within the group, DSN and its group undertakings have counted and classified the categories of data subjects involved in the processing, which are shown below:

- Employees and Crew
- Candidates

- Customers
- Suppliers
- Visitors
- Board Members (Board of Statutory Auditors, Board of Directors, etc.)

For each category of data subjects, the following information have been recorded, classified, and reported in detail in the "Register of the processing activities of d'Amico group", available at the Holding DSN and its controlled undertakings for all categories of data subjects and for the Control Authorities:

Categories of data: indicates the type of data processed for each data subject's category (art.30, c.1, let.c of the Regulation).

Legal basis of the processing: the legal basis of the processing is constituted, for the categories relating to employees, collaborators, candidates and board members, by art. 9, let. a) and b) of the Regulation, that are reported below:

a. the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

b. processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.

The legal basis of the processing is constitued, for the categories of data subjects concerning suppliers, customers and prospect and visitors, by art. 6, lett. b) and c) of the Regulation, as shown below:

b. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

c. processing is necessary for compliance with a legal obligation to which the controller is subject.

Purposes of the processing: indicate the reasons or the activities inherent to the specific data processing (art. 30, c. 1, lettera b) of the Regulation).

Repository: indicates the name of the application (in cases of electronic storage) or the name of the paper archive (in cases of paper filing) used for the management of the data related to each class of data subject. The notion of application does not include work documents (ex. File MS Excel) processed by employees, which contain personal data acquired by other software used by the company.

References: : EU Regulation n. 2016/679 of April 27, 2016

Categories of recipients who contribute to the processing: indicate the Company/Structure to which personal data are disclosed, including third countries or international organisations, to which the personal data have been or will be communicated.

2.3.1. MANAGEMENT AND RETENTION OF DATA

The criteria used to determine the applicable retention period are: personal data is kept for the time (s) necessary for its purpose, (ii) necessary for the fulfillment of the existing contractual / commercial relationship, (iii) accepted by data subject and / or (iv) required by applicable laws.

The data will be kept in any case up to the limitation period of the rights deriving from the obligations assumed.

For the management and conservation of images related to the video surveillance system, please refer to Chapter 4 "*Video Surveillance*" of this document.

2.3.2. ERASURE OF THE DATA

DSN and its group undertakings promptly delete data referring to the categories of data subjects reported in this paragraph in the cases provided for in Article 17 of the Rules.

References: : EU Regulation n. 2016/679 of April 27, 2016

Employees and Crew

Categories of data	Purposes of the processing	Legal basis	Modalities	
			Electronic	Paper
Common personal data (personal data, education and culture, etc.) Data concerning health/ occupational diseases Administrative and Accounting data Wages/Union fees Professional data	*Administrative and Accountin purposes:* ▪ Personnel management (Recruitment, selection, evaluation and monitoring of staff, aptitude tests, training). ▪ Staff's legal and economic processing (calculation and payment of salaries, application of social security and welfare legislation, layoff and earnings). ▪ Compliance with legal and fiscal obligations. ▪ Requirements related to the payment of the membership fees to the trade unions or the exercise of trade union rights (management of work permits, posting of workers, etc.), health & safety. ▪ Organization, administrative management and control of business transfers ▪ Litigation management. *Banking, credits and insurance purposes :* ▪ Insurance services (Civil liability, health, natural disasters, etc.).	- The data subject has given consent to the processing of his or her personal data for one or more specific purposes (ref. art. 6, lett. a of the Regulation). - processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (ref. art. 6, lett. b. of the Regulation)	- Nordic IT - IT2 - Sharepoint - Zantaz - Tagetik - DUALOG - OMNIA (On-board personal database managed by Sirius Ship Management for handling payments and data, and officers, captains and machine managers' paper evaluations). - Exchange Server. - HRM (software for the management of the Group's human resources.	- Paper archive, located at HR Dept. of the Holding Company and local archives l in Group's international Headquarters

References: : EU Regulation n. 2016/679 of April 27, 2016

Organisation which data are transferred to:	Identification details of recipients of personal data
Group companies	d'Amico Società di Navigazione S.p.A. and its group undertakings located in the following Non-EU countries: Principality of Monaco, Singapore, India, Morocco, USA and Liberia
External companies	Ernst Young for payroll service, ADP for USA.

References: : EU Regulation n. 2016/679 of April 27, 2016

Candidates

Categories of data	Purposes of the processing	Legal basis	Modalities	
			Electronic	Paper
Common personal data (personal data, education and culture, etc.) Particular data (e.s. health data, if present in the CV)	*Administrative and Accountin purposes*: ▪ Acquisition and CV screening ▪ CV evaluation ▪ Performing interview. ▪ Management of pre-employment obligations	- The data subject has given consent to the processing of his or her personal data for one or more specific purposes (ref. art. 6, lett. a of the Regulation). processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (ref. art. 6, lett. b. of the Regulation)	Database CV site Internet Sharepoint[3] Exchange Server Nordic IT IT2 Zantaz Tagetik DUALOG	Paper archive at the HR Department of DSN.

Organisation which data are transferred to:	Identification details of recipients of personal data
Group companies	d'Amico Società di Navigazione S.p.A. and and its group undertakings, located in the following Non-EU countries: Principality of Monaco, Singapore, India, Morocco, USA and Liberia
External companies	n.a.

[3] It is specified that the database is managed by HR Group and HR Local Manager or more generalist role. There are two profiles: admin on ROMA HR and Communication and recruiter Dublin and Singapore.

References: : EU Regulation n. 2016/679 of April 27, 2016

Customers

Categories of data	Purposes of the processing	Legal basis	Modalities	
			Electronic	Paper
Common personal data (personal data, education and culture, etc.) Data aimed at detecting the risk of financial solvency and of illicit or fraudulent behavior Administrative and Accounting data	*Administrative and Accountin purposes:* ▪ Compliance with legal and fiscal obligations . ▪ Customers management (customers' administration; administration of contracts, orders, shipments and invoices; reliability and solvency control). ▪ Litigation management (breaches of contract, warnings, transactions, debt collection, arbitration, judicial disputes). ▪ Internal control services (on security, productivity, quality of services, integrity of assets). ▪ Planning and control of economic and financial data. *Banking, credits and insurance purposes:* ▪ Accounting management or treasury.	- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (ref. art. 6, lett. b. of the Regulation)	- ERP Shipnet - ERP IMOS - Nordic IT - Virtustream - Zantaz - Tagetik - DUALOG - Exchange Server	- Paper archive at Accounting Department of DSN.

Organisation which data are transferred to:	Identification details of recipients of personal data
Group companies	d'Amico Società di Navigazione S.p.A.and its group undertakings
External companies	n.a.

References: : EU Regulation n. 2016/679 of April 27, 2016

Suppliers[4]

Categories of data	Purposes of the processing	Legal basis	Modalities	
			Electronic	Paper
Common personal data (personal data, education and culture, etc.) Administrative and Accounting data	*Administrative and Accountin purposes* : ▪ Compliance with legal and fiscal obligations . ▪ Suppliers management (suppliers' administration; administration of contracts, orders, shipments and invoices; reliability and solvency control). ▪ Planning and control of economic and financial data. *Banking, credits and insurance purposes* : ▪ Accounting management or treasury.	- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (ref. art. 6, lett. b. of the Regulation)	- ERP Shipnet - ERP IMOS - Nordic IT - Virtustream - Zantaz - Tagetik - DUALOG - Exchange Server.	- Paper archive at Purchasing Department of DSN.

Organisation which data are transferred to:	Identification details of recipients of personal data
Group companies	d'Amico Società di Navigazione S.p.A., d'Amico Shipping Singapore Pte Ltd, ISHIMA Pte Ltd
External companies	n.a.

[4] They also include the construction sites for the construction of new ships (Vietnam and Japan).

References: : EU Regulation n. 2016/679 of April 27, 2016

Visitors

Categories of data	Purposes of the processing	Legal basis	Modalities	
			Electronic	Paper
Common personal data (personal data, education and culture, etc.)	*Finalità amministrativo-contabili*: ▪ Access management. ▪ Security protection.	- The data subject has given consent to the processing of his or her personal data for one or more specific purposes	- n.a.	- Paper entry register.

Organisation which data are transferred to:	Identification details of recipients of personal data
Group companies	d'Amico Società di Navigazione S.p.A. and its group undertakings
External companies	n.a.

References: : EU Regulation n. 2016/679 of April 27, 2016

Board Members

Categories of data	Purposes of the processing	Legal basis	Modalities	
			Electronic	Paper
Common personal data (personal data, education and culture, etc.) Adiministrative and accounting data	*Administrative and Accountin purposes*: ▪ evaluation of the suitability of the profile with respect to the position held. ▪ formalization and management of offices and related payments linked to fees / reimbursement of expenses. ▪ fulfillment of administrative, insurance and tax obligations. ▪ management of contentious and pre-contentious.	✓ The data subject has given consent to the processing of his or her personal data for one or more specific purposes (ref. art. 6, lett. a of the Regulation). ✓ processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (ref. art. 6, lett. b. of the Regulation)	- Multipartner - Nordic IT - IT2 - Zantaz - Tagetik - DUALOG - Exchange Server	- Paper archive at the Legal&Insurance Department of DSN.

Organisation which data are transferred to:	Identification details of recipients of personal data
Group companies	d'Amico Società di Navigazione S.p.A. and and its group undertakings, located in the following Non-EU countries: Principality of Monaco, Singapore, India, Morocco, USA and Liberia
External companies	n.a.

References: : EU Regulation n. 2016/679 of April 27, 2016

2.4. ROLES AND RESPONSABILITIES IN THE PRIVACY FIELD

In order to complete the definition of the privacy model of the Group, roles and responsibilities have been settled, as shown below.

2.3.1. DATA CONTROLLER

As Data Controllers, DSN and its group undertakings have to comply with the obligations of the Regulation and have the following responsabilities:

- To implement appropriate technical and organizational measures to ensure, and be able to demonstrate, that the processing is carried out in accordance with the Regulation. These measures are reviewed and updated as necessary;
- To comply to the codes of conduct (see art. 40) or certification mechanisms (see art. 42) in order to demonstrate compliance with the obligations set out in the Regulation;
- To appoint, in writing, where applicable, a representative established in the European Union (see Art.27);
- To identify and appoint the processors (see art. 28 and art. 29);
- To cooperate, on request, with the Supervisory Authority in the performance of its tasks (see art. 31);
- To notify, in the event of a violation of personal data, the competent Supervisory Authority of the violation pursuant to Article 55 without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the violation of personal data is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the Supervisory Authority is not made within 72 hours, it should be accompanied by the reasons for the delay (see Article33);
- To demonstrate that the data subject has given its consent to the processing of its personal data (see art 7);
- To ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data (see art. 38);
- To support the data protection officer in performing its tasks (see art. 39), by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge (see art. 38);

- To ensure that the data protection officer does not receive any instructions regarding the exercise of its tasks (see art. 38).

2.3.2. DATA PROTECTION OFFICER (DPO) (ART. 37)

In accordance with art.37 of the Regulation, DSN has appointed as DPO at group level, in staff to Data Controller.

The appointment of the DPO has been formalized through a letter of appointment which regulates its tasks in detail; copy of this appointment letter countersigned by the DPO is filed at HR Department.

The DPO, in accordance with the provisions of art.38 of the Regulation:

- shall be involved, properly and in a timely manner, in all issues which relate to the protection of personal data; shall be provided of the necessary resources to carry out his tasks;
- cannot be removed or penalized by the Data Controller or by the Data Processor for the performance of their duties;
- directly report to the highest management level of the controller or the processor;
- may be contacted by data subjects with regard to all issued related to processing of their personal data;
- shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law;
- may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

The *governance* of the privacy management system through this figure will allow DSN and its group undertakings not only to comply with the provisions on *data protection*, but also to control the legal liability profiles deriving from the application of the *principle of accountability*.

The main tasks of DPO are reported below:

a) to coordinate and manager the privacy coordinators appointed by DSN for each company of d'Amico Group;
b) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;
c) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

d) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;
e) to cooperate with the supervisory authority;
f) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

2.3.3. PRIVACY COORDINATORS (ART.37.2)

In compliance with paragraph 2 of the art. 37 of the Regulations, DSN, in order to facilitate the coordination and management of actions aimed to compliance with the aforementioned Regulation, has appointed, for each country in the group at international level, a Privacy Coordinator.

This figure is coordinated by the DPO.

The appointment of the individual Privacy Coordinators is formalized through a letter of appointment which governs the tasks in detail; a copy of the appointment letters countersigned by the Privacy Coordinators is filed at the HR Department.

2.3.4. DATA PROCESSORS (ART. 28-29)

In accordance with art.28 of the Regulation: "*Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject*".

The Data processor (hereinafter processor) is therefore identified by the Data Controller among subjects who, by experience, ability and reliability, are able to provide a suitable guarantee of full compliance with the current provisions on processing, including the relative profile to the security of personal data managed (both with the aid of IT tools and not).

D'Amico Group has distinguished the role of Data Processor into:

- *Internal Data Processor;*
- *External Data Processor.*

2.3.4.1. INTERNAL RESPONSIBLE DATA PROCESSOR

DSN and its group undertakings, as Data Controllers, have appointed as Internal Data Processors, the Heads of the Organizational Functions, which within the scope of their duties, deal manually or with

electronic tools, personal data of which d'Amico's group is the Controller. These appointments are formalized through a letter of appointment which governs their duties in detail; a copy of the appointment letters countersigned by the internal Data Processor is filed at the group DPO structure.
Organizational changes that may have an impact on the organization of Internal Data Processors must be communicated to the DPO, which evaluates and proposes any changes to the organization to DSN.

2.3.4.2. EXTERNAL DATA PROCESSOR

DSN and its group undertakings, as Data Controllers, have appointed, as External Data Processors, companies and professionals who provide services to the individual companies of d'Amico group, which, to the scope of the appointment received from the companies of the d'Amico group, deal manually or with electronic means, personal data of which the d'Amico group is the Controller.

DSN outlined two different types of external data processor, differentiating this role in:
a) External Data Processor within the Group;

b) External Data Processor outside the Group.

These appointments are formalized by means of a letter of appointment on the basis of the processings performed by each external data processor which regulates their duties; a copy of the appointment letters countersigned by the Manager is filed at the group DPO structure.

Organizational changes that may have an impact on the organization of external Privacy Managers must be communicated to the DPO that evaluates and proposes to the Data Controller any changes to be made to the organization.

2.3.5. PERSONS IN CHARGE OF THE PROCESSING

DSN and its group undertakings, as Data Controllers, have identified different Classes of operators, which include all the employees and collaborators of the various companies in the Group who, as part of their duties, deal manually or with electronic means, personal data of which DSN and its group undertakings are Controllers.

These designations are formalized through a special letter that governs their duties; copies of the designation letters countersigned for inspection by the operators are archived and stored at the group DPO structure.

References: : EU Regulation n. 2016/679 of April 27, 2016

2.3.6. SYSTEM ADMINISTRATORS

DSN and its group undertakings, as Data Controllers, have appointed as System Administrators, employees and collaborators with particular duties and responsibilities in the management and maintenance of business applications and technological infrastructure, pursuant to provided for in point 2, letter c. of the Measure referred to in par. 1.2 which provides *"for the identification data of natural persons in the role of system administrators, with the list of the functions attributed to them, must be reported in an internal document to be kept up to date and available in the event of investigations by the Italian DPA"*.

References: : EU Regulation n. 2016/679 of April 27, 2016

3. RISK ASSESSMENT (art.32)

This chapter concern the risk assessment carried out between the end of 2016 and the beginning of 2017 by DSN, for each company of d'Amico Group and aimed to:

- detecting the technical and organizational security measures in place within the d'Amico Group with regard to the security of personal data;
- evaluate relative adequacy;
- define any measures to be implemented to ensure compliance with the legislation on the protection of personal data.

The elements for risk assessment, in compliance with the provisions of the Regulations, are the following:

a) existence of procedures for anonymization and pseudonymization of personal data;
b) ability to ensure on a permanent basis the confidentiality, integrity, availability and resilience of processing systems and services;
c) ability to promptly restore the availability and access of personal data in the event of a physical or technical incident;
d) existence of a procedure for testing, verifying and regularly assessing the effectiveness of technical and organizational measures in order to guarantee the security of the treatment.

It is important to specify, in order to complete the scenario, that the scope of the risk analysis is referring exclusively to personal data and to the related processing that the Data Processors perform in the context of the activities carried out within the d'Amico Group.

In the following paragraphs, the used methodology is presented as well as the results of the analysis and the synthesis of the detected criticalities.

3.1. RISK ASSESSMENT FRAMEWORK

The reference methodology used is refers to the Guidelines of the main international standards for Risk Assessment and the security of the informative systems (ISO 27001: 2005 and ISO 27005), and aims to produce comparable and reproducible results over time.

The standard methodological steps followed for the implementation of the activities, are the following:

- Identification of the risks
- Risk analysis and assessment.

The methodological steps, in detail, is report below.

3.1.1. IDENTIFICATION OF THE RISKS

Risk identification takes place through a structured procedure that focuses on the resources to protect.

This phase is divided into the following four sub-phases:

1. identification of resources;
2. identification of harmful events and risk factors;
3. classification of risks;
4. detection of existing security measures.

Below is a breakdown of the objectives and activities of each sub-phase:

3.1.1.1 IDENTIFICATION OF RESOURCES

The sub-phase allows the identification of all the informative resources of the Companies, the personal data managed and the related processing under analysis. The information are acquired through the carrying out of interviews to the referents of each interested structure.

3.1.1.2. IDENTIFICATION OF HARMFUL EVENTS AND RISK FACTORS

The sub-phase allows to identify, for each of the previously identified resources, all the harmful events capable of compromising the requirements of integrity, confidentiality, availability and reliability of personal data. Subsequently, for each event, risk factors should be identified, therefore how the procedures causing the damaging events can occur for each resource under examination.

The identification of harmful events and risk factors takes into consideration both the specific nature of the organization and the infrastructure of the Company, as well as the indications provided by the Supervisory Authority.

3.1.1.3. CLASSIFICATION OF THE RISKS

The sub-phase allows to define the macro categories of risks analysed, as shown below:

- Risks inherent to information systems and data security, in turn distinguished in:
  - Physical risks: risks related to areas and premises where communication systems and devices are located, risks related to access of people in the same premises, risks related to the integrity and availability of ICT systems and devices (lack of protection of the premises, lack of access control, etc.).

- Logical risks: risks related to the integrity, confidentiality and availability of data.
- Transmission risks: risks related to the security of data transmissions.

- Compliance risks: risks related to failure to comply with the various requirements set out in the Regulations (ex. appointment of processors and persons in charge of processing, preparation of information and related requests for authorization for processing, training, etc.).

3.1.1.4. DETECTION OF EXISTING SECURITY MEASURES

The sub-phase allows to identify the existing protection measures for risk mitigation. In this sense it is necessary to take into account both information security measures and physical and organizational security measures.

3.1.2. RISK ANALYSIS AND ASSESSMENT

This phase is characterized by the measurement of the so-called "residual risk level", which means the residual risk assessed after the assessment of the control system and the actions taken to mitigate the inherent risk. This phase is achieved through the following three sub-phases:

1. determination of the inherent risk level
2. determination of the residual risk level
3. identification and assessment of options to treat the risks

3.1.2.1. DETERMINATION OF THE LEVEL OF INHERENT RISK

The inherent risk is generally defined as the risk connected to an activity and / or to a business process, regardless of the level of control present in those areas.

The factors that determine the level of inherent risk are the impact, i.e. the relevance of the consequences caused by the harmful event and the probability, or the possibility that the harmful event occurs in a reference period.

Tables n.1 and n.2 present, respectively, the values of impact and likelihood assigned in the assessment.

Table 1 – Assignment of impact values

Impact	Index	Meaning
Low	10	The effects of the harmful event are limited from every point of view: legal, functional and of reputation.
Medium	50	The effects of the harmful event are circumscribed, with significant but sustainable consequences.

High	100	The effects of the malicious event can have serious consequences for the organization.

Table 2 – Assignment of likelihood values

Likelihood	Index	Meaning
Low	0,1	The event could occur at most once in a period of more than 10 years.
Medium	0,5	The event could occur several times over a period of 10 years, but not annually.
High	1	The event could occur at least once in a year

The extent of the inherent risk is therefore given by the relationship between the probability of occurrence of the event and the potential negative impact produced.

Tables 3 and 4 present, respectively, the assessment and description of inherent risk.

Table 3 – Assessment of inherent risk

Risk level		Likelihood		
		Low	Medium	High
Impact	Low	1	5	10
	Medium	5	25	50
	High	10	50	100

Table 4 – Description of inherent risk

Risk level	Value	Meaning
Low	< 10	The inherent risk level is negligible and it is not necessary to prepare control measures.
Medium	>= 10 and < 50	The level of inherent risk is not negligible, and risk mitigation measures should be prepared.
High	>= 50	The level of inherent risk is high, and it is necessary to prepare control measures for risk mitigation.

References: : EU Regulation n. 2016/679 of April 27, 2016

3.1.2.2. DETERMINATION OF THE LEVEL OF RESIDUAL RISK

The residual or mitigated risk is generally defined as the risk that remains after the assessment of the control system. The extent of this risk is determined by the combination of entities of the inherent risk and assessment of the adequacy of the controls (or protection measures) in place, as shown in Table 5.

Table 5 – Determination of residual risk

Residual risk		Control assessment		
		Adequate	Partial	Not adequate
Inherent Risk	Low	Low	Low	Medium
	Medium	Low	Medium	High
	High	Medium	High	High

3.1.2.3. IDENTIFICATION AND ASSESSMENT OF THE OPTIONS FOR TREATING RISKS

At the end of the sub-phase, if there is a medium or high level of residual risk, it is possible to identify further safety measures, in order to reduce the risk to an acceptable level.

Among the available options, it is possible to accept risks consciously and objectively, in compliance with company policies. In alternative, it is possible to decide whether to avoid the risk, cancelling the risk factor or giving up a certain resource.

Finally, it can be possible to decide to transfer the risk to another person, such as an insurance or a provider.

3.2. ASSESSMENT RESULTS

The following paragraphs show the results of the risk analysis carried out.

3.2.1. IDENTIFICATION OF THE RISKS

In order to proceed with the identification of the risks, the organization and infrastructure of the Informative Systems of the d'Amico Group have been examined, which is shown below.

3.2.2. DETECTION OF THE TECHNOLOGICAL AND APPLICATION INFRASTRUCTURE

The management of the ICT infrastructure of the d'Amico Group is delegated to Virtustream provider based in London, and is governed by a IaaS (Infrastructure-as-a-Service) contract.

The list of the IT provider's main servers, hosted in the Data Centre of London (UK-DC), is the following:

- domain controller;
- file server;
- data server and applications;
- e-mail server;
- backup server;
- sftp server.

All virtual machines hosted in the Virtustream Data Centre in London (UK-DC) are redundant in the Virtustream Data Centre in Amsterdam (NL-DC).

The connection with d'Amico servers is assured by an MPLS line, managed by the BT provider, which divides the following Group locations: Rome, Genoa, Dublin, Monaco, Singapore, Luxembourg, London, Stamford, Mumbai, Manila, and is redundant through the use of a backup line.

The connection to the telematics network is made via firewalls that constantly monitor incoming and outgoing Internet traffic, with the aim of:

- managing internet access and registering logs;
- controlling web traffic;
- Antivirus;
- Anti-Spyware.

The workstations located at d'Amico offices are connected to the company LAN, allowing the use of network units with limited access to the personnel belonging to the Company Departments, network units with access restricted to individual employees and network units for document exchange.

An antivirus is installed on the servers and on the clients, configured to be continually and automatically updated on every single client with the latest releases of the manufacturer. Users cannot block or cancel the virus update and scan.

References: : EU Regulation n. 2016/679 of April 27, 2016

Figure 1 shows the articulation of d'Amico Group's technological infrastructure:

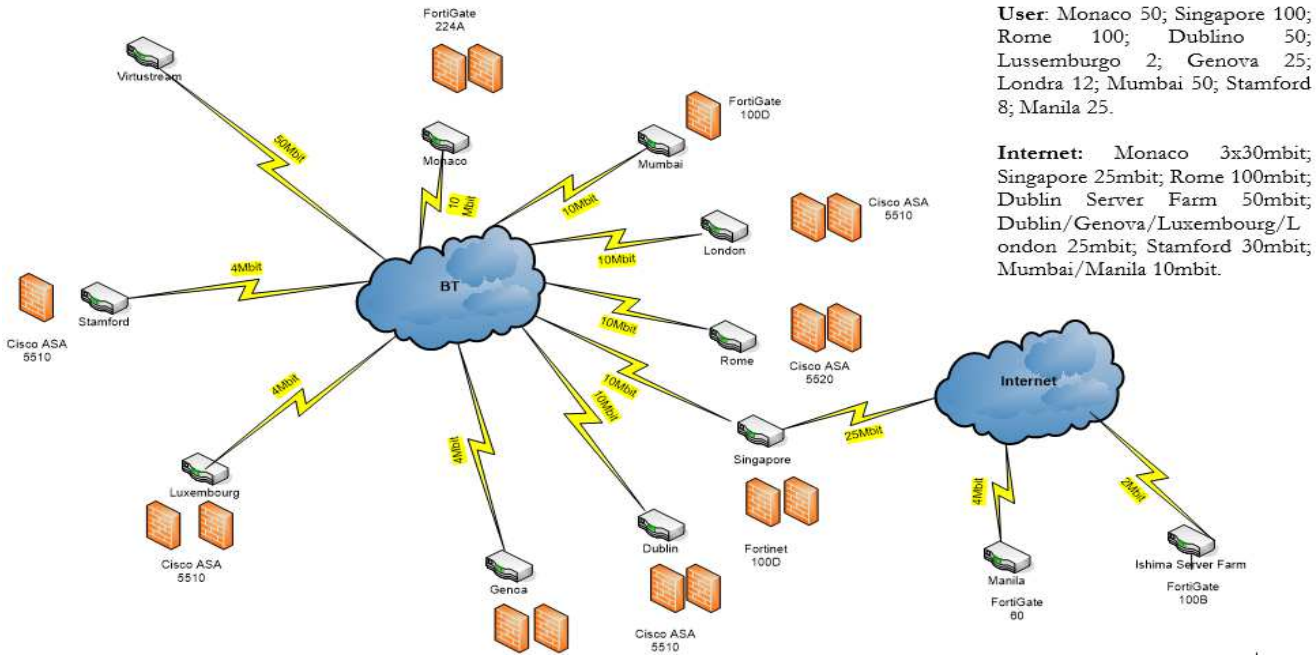


Figure 1 – d'Amico Group's technological infrastructure

To complete the sub-phase, in the following table is reported a list of the applications and the related categories of data subjects present in DSN and its group undertakings, which fall within the scope of the Regulation.

Applications	Description	Data subjects involved
SHIPNET	ERP	Customers Suppliers
INTERNATIONAL MARITIME OPERATION SYSTEM (IMOS)	ERP Chartering and Operations management	Customers Suppliers
MARK V	Access management system for e-mail	ALL
DUALOG	Digital platform for managing on-board e-mail	ALL
MIMECAST	Mail continuity system (temporary back up of e-mail)	ALL
IT2	The system is managed by: - Finance Dept. for treasury management of the Group - ICT Dept. for the management of credentials.	Employees Customers Suppliers
SHAREPOINT	Content Management System (CMS) software platform for managing the portal of the company	Employees
ZANTAZ	Mail storage system	Employees, Customers

		Suppliers and Boards Members
WATCHKEEPER	System for monitoring on-board personnel (eg working hours by on-board personnel)	Crew
TNSJ TRAVEL	Application for travel management	Employees
WEB SITE – APPLICATION MANAGEMENT	Application acquisition system	Candidates
Exchange Server	E-mail management system	ALL

3.2.3. MAIN RISKS AND RELATED SECURITY MEASURES

The following tables show the main harmful events for data security and the assessment of possible consequences and severity, in relation to the following electronic contexts and tools used:

- Data backup;
- Operators' behavior;
- Incident management;
- Logs collection and monitoring;
- ICT Physical security;
- Security of the Group's Data Center;
- Logical security of accesses;
- Data security;
- Network security;
- Application security;
- Logical security;
- Workstation security.

References: EU Regulation no. 2016/679 of April 27, 2016

3.2.4. RISK MATRIX

Context	Event	Risk factors	Impact	Likelihood	Inherent risk	Protection measures in place	Control assessment	Residual risk
Data backup	Removal and theft of backups	- Inadequate storage location	M	L	L	- ITG-02 Global ICT Security Policy - ITG-10 Backup - WI-ITG-02 Back-up Quick Reference - Contract Cloud Providers	Adequate	Low
Data backup	Destruction and data loss	- Unavailability of data	M	M	M	- ITG-02 Global ICT Security Policy - ITG-10 Backup - WI-ITG-02 Back-up Quick Reference - Contract SLA Cloud Providers	Partial	Medium
Data backup	Litigation with providers	- Unavailability of data	H	L	M	- ITG-02 Global ICT Security Policy - ITG-10 Backup - WI-ITG-02 Back-up Quick Reference - Contract SLA Cloud Providers	Partial	Medium
Operators' behavior	Unauthorized accesses to company systems	- Inadequate storage location	L	L	L	- ITG-01 Acceptable use of ICT Resources Policy V.2.01 - Adoption of strong authentication rules ITG-09 Users Accounts - WI-ITG-04 Users Authorization register	Adequate	Low

References: EU Regulation no. 2016/679 of April 27, 2016

Context	Event	Risk factors	Impact	Likelihood	Inherent risk	Protection measures in place	Control assessment	Residual risk
Operators' behavior	Loss of data contained in company systems	- Lack of awareness, carelessness by employees	L	L	L	- ITG-01 Acceptable use of ICT Resources Policy V.2.01 - ITG-02 Global ICT Security Policy - ITG-10 Backup - WI-ITG-02 Back-up Quick Reference - PIM	Adequate	Low
Operators' behavior	Theft of tools containing data	- Omitted custody	L	L	L	- Code of Ethics - 231 Model - Social Media Policy - PIM	Adequate	Low
Incident management	Malfunction, unavailability of applications	- Inadequate monitoring	M	M	M	- ITG-07 ERP Emergency Change - Incident Log and Incident Report (2 time a year)	Partial	Medium
Systems monitoring	Malfunction, unavailability of applications	- Inadequate detection of exceptions, malfunctions and events relating to the system	M	L	L	- ITG-07 ERP Emergency Change - Yearly Penetration Test - Quarterly Risk Report - Weekly Network Threats Report - Half Year Administrator Log Report - Bridge and NAV Network Security - Risk Assessment	Adequate	Low
Logs collection and monitoring	Log manipulation	- Inadequacy of the authentication systems in which the logs reside	L	L	L	- ITG-01 Acceptable use of ICT Resources Policy V.2.01 - Adoption of strong authentication rules ITG-09 Users Accounts	Adequate	Low

References: EU Regulation no. 2016/679 of April 27, 2016

Context	Event	Risk factors	Impact	Likelihood	Inherent risk	Protection measures in place	Control assessment	Residual risk
						- WI-ITG-04 Users Authorization register		
Logs collection and monitoring	Fraudulent behavior by the System Administrators	- Inadequate monitoring of the operations of the System Administrators	H	L	M	- Half Year monitoring of system administrator access logs - WI-ITG-03 Competence Chart - Code of Ethics	Partial	Medium
Physical security	Unauthorized access to company's buildings	- Absence of environmental protection measures in areas containing sensitive or critical information - Human errors in the management of physical security	M	L	L	- Protection of the offices - Entry registration (where applicable) - Reception Service (where applicable)	Adequate	Low
Physical security	Unauthorized access to restricted access departments	- Inadequate management of access to restricted access departments (ex. CED) - Violation of intruder systems	M	L	L	- Code of Ethics - Badge (where applicable) - Locked doors (where applicable)	Adequate	Low
Physical security	External and environmental threats that could cause an indisposition of the equipment	- Inadequate physical protection from natural disasters, malicious attacks or incidents.	M	L	L	- Antivirus (centralized) - Firewall - UPS - Disaster Recovery Plan - Redundancy of the servers in	Adequate	Low

References: EU Regulation no. 2016/679 of April 27, 2016

Context	Event	Risk factors	Impact	Likelihood	Inherent risk	Protection measures in place	Control assessment	Residual risk
						which the applications and data reside - Contract Cloud Providers		
Security of Group's Data center	Destructive - natural or artificial, malicious, accidental or due to negligence - events	- Lack of environmental protection measures - Lack of continuity measures	L	L	L	- Contract Cloud Providers	Adequate	Low
Group Data center's security	Failure of complementary systems (electrical system, air conditioning, ...)	- Lack of power supply system - Overheating of equipment	L	L	L	- Periodic maintenance of the system - UPS	Adequate	Low
Group Data center's security	Human errors in the management of physical security	- Lack of awareness, carelessness	L	L	L	- ICT Governance - Internal training and awareness	Adequate	Low
Logical security of accesses	Access to data by unauthorized personnel	- Absence of a process for the assignment or revocation of access rights for all types of users and for all systems and servers in line with the position held - Absence of an access control policy	M	L	L	- ITG-09 Users Accounts - WI-ITG-04 Users Authorization register - Monitoring of failed access attempts	Adequate	Low

References: EU Regulation no. 2016/679 of April 27, 2016

Context	Event	Risk factors	Impact	Likelihood	Inherent risk	Protection measures in place	Control assessment	Residual risk
Logical security of accesses	Loss of confidentiality of passwords to access to systems	- Inadequate security level of the Password	L	L	L	- ITG-09 Users Accounts - WI-ITG-04 Users Authorization register - Adoption of Strong Authentication rules in line with international best practices (> 8 characters, alphanumeric, must not related to personal information, former name, for example, date of birth, etc., change password every 90 days)	Adequate	Low
Data security	Data theft	- Lack of awareness, carelessness	L	L	L	- Encrypted data in both storage clouds and on the network	Adequate	Low
Data security	Unauthorized access to data from the Virtustream Provider	- Absence of a policy on the use, protection and durability of encryption keys	M	L	L	- Encryption of personal data	Adequate	Low
Network security	Data loss due to errors in storage media	- Lack of backups	M	L	L	- ITG-02 Global ICT Security Policy - ITG-10 Backup - WI-ITG-02 Back-up Quick Reference	Adequate	Low
Network security	Virus, Worm, Malware attacks	- Lack of a software to contrast malicious code	M	L	L	- Firewall - Antivirus - Antispam - Ethical hackers campaign - Reduced user privileges	Adequate	Low

References: EU Regulation no. 2016/679 of April 27, 2016

Context	Event	Risk factors	Impact	Likelihood	Inherent risk	Protection measures in place	Control assessment	Residual risk
						- ITG-11 IS Configurations		
Network security	Processing errors	- Incorrect management, modification or update of programs	M	L	L	- Test environment separate from production environment - Preliminary test of updates or evolutionary changes ITG-07 ERP Emergency Change	Adequate	Low
Application security	Malfunction, unavailability or degradation of the equipment	- Network architecture with reduced reliability - lack of updates	L	L	L	- Server redundancy - Periodic update of infrastructure servers - Virtual Machine for remote maintenance - ITG-11 IS Configurations	Adequate	Low
Application security	Unauthorized access to informative system	- Inadequacy of the authentication systems	L	L	L	- ITG-01 Acceptable use of ICT Resources Policy V.2.01 - ITG-09 Users Accounts - WI-ITG-04 Users Authorization register	Adequate	Low
Application security	Virus, Worm, Malware attacks	- Lack of a software to contrast malicious code	M	L	L	- Firewall - Antivirus - Antispam - Reduced user privileges	Adequate	Low
Application security	Theft or loss of data	- User's unguarded equipment	L	L	L	- ITG-01 Acceptable use of ICT Resources Policy V.2.01 - Perimeter security of the offices	Adequate	Low
Logical security	Actions of virus or software capable to cause damages	- Lack of a software to contrast malicious code	H	M	H	- Antivirus - Penetration test - Yearly Penetration Test	Adequate	Medium

References: EU Regulation no. 2016/679 of April 27, 2016

Context	Event	Risk factors	Impact	Likelihood	Inherent risk	Protection measures in place	Control assessment	Residual risk
						- Quarterly Risk Report - Weekly Network Threats Report - Half Year Administrator Log Report - Bridge and NAV Network Security - Risk Assessment - Ethical hackers campaign		
Logical security	Spamming or sabotage techniques	- Insufficient security policies	L	L	L	- Antispam - ITG-01 Acceptable use of ICT Resources Policy V.2.01 - Ethical hackers campaign	Adequate	Low
Logical security	Malfunction, degradation or unavailability of applications	- Lack of updates	L	L	L	- Periodic update of SWs	Adequate	Low
Logical security	Unauthorized external accesses	- Inadequate authentication systems	L	L	L	- ITG-01 Acceptable use of ICT Resources Policy V.2.01 - ITG-09 Users Accounts - WI-ITG-04 Users Authorization register - Assess to external System Administrators via PIM	Adequate	Low
Asset management	Theft or loss of data	Data Disclosure	M	L	L	- ITG-01 Acceptable use of ICT Resources Policy V.2.01 - ITG-11 IS Configurations - Encryption of magnetic supports - Project to blocking USD On Board	Adequate	Low

References: EU Regulation no. 2016/679 of April 27, 2016

Context	Event	Risk factors	Impact	Likelihood	Inherent risk	Protection measures in place	Control assessment	Residual risk
Workstation security	Installation of software or devices for sabotage or interception of information	- Insufficient security policies	L	L	L	- Antispam - ITG-01 Acceptable use of ICT Resources Policy V.2.01	Adequate	Low
Workstation security	Destruction or loss of data	- Lack of backups	L	L	L	- ITG-01 Acceptable use of ICT Resources Policy V.2.01 - ITG-02 Global ICT Security Policy - ITG-10 Backup - WI-ITG-02 Back-up Quick Reference	Adequate	Low

References: EU Regulation no. 2016/679 of April 27, 2016

3.3. SUMMARY OF DETECTED CRITICALITIES

The following table summarizes the actions to be taken to overcome the relative criticalities for each type of residual risk assessed as "MEDIUM".

Context	Event	Risk factor	Inherent Risk	Protection measures in place	Control Assessment	Residual Risk	Answer to residual risk			
							Accepted	Reduced	Avoided	Transferred
Data backup	Destruction and loss of data	- Unavailability of data	M	- ITG-02 Global ICT Security Policy - ITG-10 Backup - WI-ITG-02 Back-up Quick Reference - Contract SLA Cloud Providers	Partial	Medium		Review of the existing backup procedure. Disaster recovery. BIA review. File system cloud.		
Incident management	Malfunction, unavailability of applications	- Inadequate monitoring	M	- ITG-07 ERP Trouble Ticketing	Partial	Medium		Monitoring of incident logs. Incident database. WorkAround.		
Logical security	Actions of virus or software capable to cause damages	- Lack of a software to contrast malicious code	H	- Antivirus - Penetration test - Yearly Penetration Test - Quarterly Risk Report - Weekly Network Threats Report - Half Year Administrator Log Report - Bridge and NAV Network Security - Risk Assessment - Ethical hackers campaign	Adequate	Medium	X			

References: : EU Regulation no.2016/679 of April 27, 2016.

3.4. FINAL CONSIDERATIONS AND ACTION PLAN

The analysis carried out shows an overall picture of the substantial adequacy of the control system in place within the d'Amico Group, which ensures adequate protection of personal data, in compliance with the provisions of Regulation 679/2016. The analysis highlighted, however, some areas of improvement on which it is recommended to intervene.

In relation to "Data Backup", "Incident Management" and "Log and Monitoring Collection" the d'Amico Group has prepared a response to the residual risk, in order to reduce it, planning the following actions:

- *review of the Back-up, IS Configurations, Disaster Recovery Documentations.*
- *document data security On Shore and On Board.*
- *monitor of the Incident Database and Incident Workaround Logs.*
- *log collection and half year monitoring of system administrator access logs.*
- *set contractual security clauses with third parties providers.*

In relation to "Logical Security", d'Amico's Group accepted the relative risk.

3.5. REFERRED DOCUMENTS

✓ 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: : EU Regulation no.2016/679 of April 27, 2016.

4. VIDEO SURVEILLANCE

DSN and the subsidiary DSI, in relation to the business activities and the requirements for the protection of the company's safety and assets, have requested the competent Authorities for the necessary installation of video surveillance systems within the following operational offices:

- Genoa, Via dei Marini n. 53 - Torre Shipping Scala A
- Rome, Corso d'Italia 35b

Below are the details of the Authorization Provisions issued by the competent Authorities and the details of the installed video surveillance systems.

4.1. VIDEO SURVEILLANCE SYSTEMS OF D'AMICO SOCIETÀ DI NAVIGAZIONE S.P.A.

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

With the Decree n. 154 of 03/12/2012, DSN received from the Ministry of Labor and Social Policies - Territorial Department of Labor of Genoa, the authorization to install a video surveillance system at the company's headquarters, located in Via dei Marini n. 53 - Torre Shipping Scala A, in Genoa.

The video surveillance system consists of n. 2 internal fixed cameras and n. 1 video recording unit.

Rome, Corso d'Italia 35b

With Provision Prot. N. 85023 dated 13/09/2013, DSN received from the Ministry of Labor and Social Policies - Territorial Labor Department of Rome, the authorization to install a video surveillance system at the company's headquarters, located in Corso d'Italia Italy 35b in Rome.
The video surveillance system consists of n. 21 internal fixed cameras, n. 3 external fixed cameras, n. 1 video recording system and n. 3 monitors located as follows:

n. 21 telecamere, distribuite nelle seguenti aree:

- n. 2 cameras at the basement;
- n. 5 cameras at ground floor;
- n. 7 cameras at first floor;
- n. 3 cameras at second floor;
- n. 6 cameras at third floor;

n. 3 cameras, located in the following areas:

- n. 2 cameras in the parking area;

- n. 1 camera at the entrance of the building;
- n. 1 video-recording system installed at second floor.

n. 3 monitor located in the following areas:

- n. 1 monitor at ground floor;
- n. 1 monitor at first floor;
- n. 1 monitor at third floor.

In relation to the Authorization received, d'Amico Società di Navigazione S.p.A. has formalized the relevant appointments of the Processors for these surveillance systems and to designate the relevant classes of operators.

The following are the names of the appointed data processors and the related purposes of the processings.

Internal Data Processor	Structures where the cameras are located	Data subjects	Purposes of the processing
Francesco Rotundo	Outdoor area: parking and hallway Internal area: basement, ground floor, first floor, second floor and third floor	All the categories of data subjects that access the Genoa and Rome offices, including employees	Purposes of preventing theft, damage or vandalism and fire prevention as well as the safety of workers.

For more details, refer to the specific information available at the headquarters of d'Amico Società di Navigazione S.p.A.

4.2. VIDEO SURVEILLANCE SYSTEMS OF D'AMICO SHIPPING ITALIA S.P.A.

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

With Decree n. 157 of 17/12/2012, d'Amico Shipping Italia S.p.A. received from the Ministry of Labor and Social Policies - Genoa Territorial Labor Department, the authorization to install a video surveillance system at the company's headquarters, located in Via dei Marini n. 53 - Torre Shipping Scala A in Genoa. The video surveillance system consists of n. 2 internal fixed cameras and n. 1 video recording unit.

Rome, Corso d'Italia 35b

With Provision Prot. N. 95430 of 08/10/2013, DSI received from the Ministry of Labor and Social Policies - Territorial Labor Department of Rome, the authorization for the installation of a video surveillance system at the company's headquarters, located in Corso d ' Italy 35b in Rome.

References: : EU Regulation no.2016/679 of April 27, 2016.

The video surveillance system consists of n. 21 internal fixed cameras, n. 3 external fixed cameras, n. 1 video recording system and n. 3 monitors located as follows:

n. 21 cameras, located in the following areas:

- n. 2 cameras at the basement;
- n. 5 cameras at ground floor;
- n. 7 cameras at first floor;
- n. 3 cameras at second floor;
- n. 6 cameras at third floor;

n. 3 cameras, located in the following areas:

- n. 2 cameras in the parking area;
- n. 1 camera at the entrance of the building;

n. 1 video recording system at second floow;

n. 3 monitor dislocati nelle seguenti aree:

- n. 1 monitor at ground floor;
- n. 1 monitor at first floor;
- n. 1 monitor at third floor.

In relation to the Authorization received, d'Amico Shipping Italia S.p.A. has formalized the relevant appointments of the data processors for these surveillance systems and to designate the relevant classes of operators.

The names of the appointed Processor and the related purposes of the processings are shown below.

Internal data processor	Structures where the cameras are located	Data subjects	Purposes of the processing
Francesco Rotundo	Outdoor area: parking and hallway Internal area: basement, ground floor, first floor, second floor and third floor	All the categories of data subjects that access the Genoa and Rome offices, including employees	Purposes of preventing theft, damage or vandalism and fire prevention as well as the safety of workers.
Paola Cappabianca	Outdoor area: parking and hallway Internal area: basement, ground floor, first floor, second floor and third floor	All the categories of data subjects that access the Genoa and Rome offices, including employees	Purposes of preventing theft, damage or vandalism and fire prevention as well as the safety of workers.

For more details, please refer to the specific information, available at the headquarters of d'Amico Shipping Italia S.p.A..