References: Reg EU 2016/679

GROUP OF UNDERTAKINGS d'Amico

Holding

d'Amico Società di Navigazione S.p.A.

GROUP PRIVACY REGULATION EX REGULATION UE 679/2016

(Containing the "BINDING CORPORATE RULES")

INDEX

PREMISE

D'Amico Società di Navigazione S.p.A. (hereinafter DSN) and the Companies *in scope or out of scope* (as declined into "Annex 1") process personal data of the following data subjects:

- Employees and Crew;
- Candidates;
- Customers and Prospect;
- Suppliers;
- Visitors;
- Board Members (Board of Statutory Auditors, Board of Directors, exc.);

In compliance with lawfulness, fairness and trasparency principles established by Regulation 2016/679, hereinafert "Regulation".

In order to ensure that the processing of personal data of the above mentioned data subjects was carried out in compliance with the principles established by current legislation, DSN and the Companies *in scope and out of scope*, implemented a system for privacy management, illustrated into Annex 1.

To complete the Group Privacy Model, DSN has approved these Binding Corporate Rules, which represent one of the Regulation compliance tools, with special reference to the case of "*transfer of personal data outside European Union*" regarding the following categories of data subjects:

- Employees and Crew
- Candidates
- Board Members

1. INTRODUCTION

These Binding Corporate Rules represent the unilateral tool through which d'Amico Società di Navigazione S.p.A., hereinafter DSN, as Holding of d'Amico Group, intends to provide the adequate guarantees required for the transfer of data within the Group to third countries, to the identified categories of data subjects (employees and crew), candidates and board members. These Binding Corporate Rules are approuved in absence of adequacy decisions deriving from Chapter V "*Transfer of personal data to third countries or international organisation*".

These provisions set the rules for the correct application of the policies about data protection. These provisions are legally binding for each company of the Group, including all group's employees.

These rules ensure compliance with the data protection requirements and with the data subjects' rights, who are expressly conferred with rights related to the processing of personal data referred to them.

It is specified that DSN defined the form, the content and the field of these Binding Corporate Rules, in accordance with the provisions of Chapter V, Art. 47 EU Regulation 2016/679, called "Binding corporate rules".

1.1. Definitions

The Regulation proposes the "*essential vocabulary*" regarding to the scope of data protection.

The most important definitions are shown below.

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.

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

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

1.2. Document Structure

The structure of this document, in accordance with the provisions of the Regulation, is the following:

1. The structure and the contact details of DSN and its controlled undertakings.
2. The categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question.
3. The legally binding nature of these rules, both internally and externally.
4. The explication of the general data protection principles, in particular purposes limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules.
5. The rights of data subjects in regard to the processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including

profiling in accordance with Article 22, the right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;

6. The acceptance by DSN and its controlled undertakings of liability for any breaches of the binding corporate rules by any member concerned not established in the Union.
7. How the information on Binding Corporate Rules is provided to the data subjects.
8. The tasks of any data protection officer designated of the monitoring compliance with the binding corporate rules within the group, as well as monitoring training and complaint-handling.
9. The complaint procedures.
10. The mechanisms within the group for ensuring the verification of compliance with the binding corporate rules. Such mechanisms include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to Data Protection Officer, to the board of Directors and should be available upon request to the competent supervisory authority.
11. The mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority.
12. The cooperation mechanism with the supervisory authority to ensure compliance by any member of the group, in particular by making available to the supervisory authority the results of the internal control activities.
13. The mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings, is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules.
14. The appropriate data protection training to personnel having permanent or regular access to personal data.

1.3. Purposes and scope

The application field of these Binding Corporate Rules is the processing of personal data relating to the following data subject categories:

- Employees and Crew
- Candidates
- Board Members

carried out by undertakings of the group, which could be transferred outside European Union for contractual management purposes.

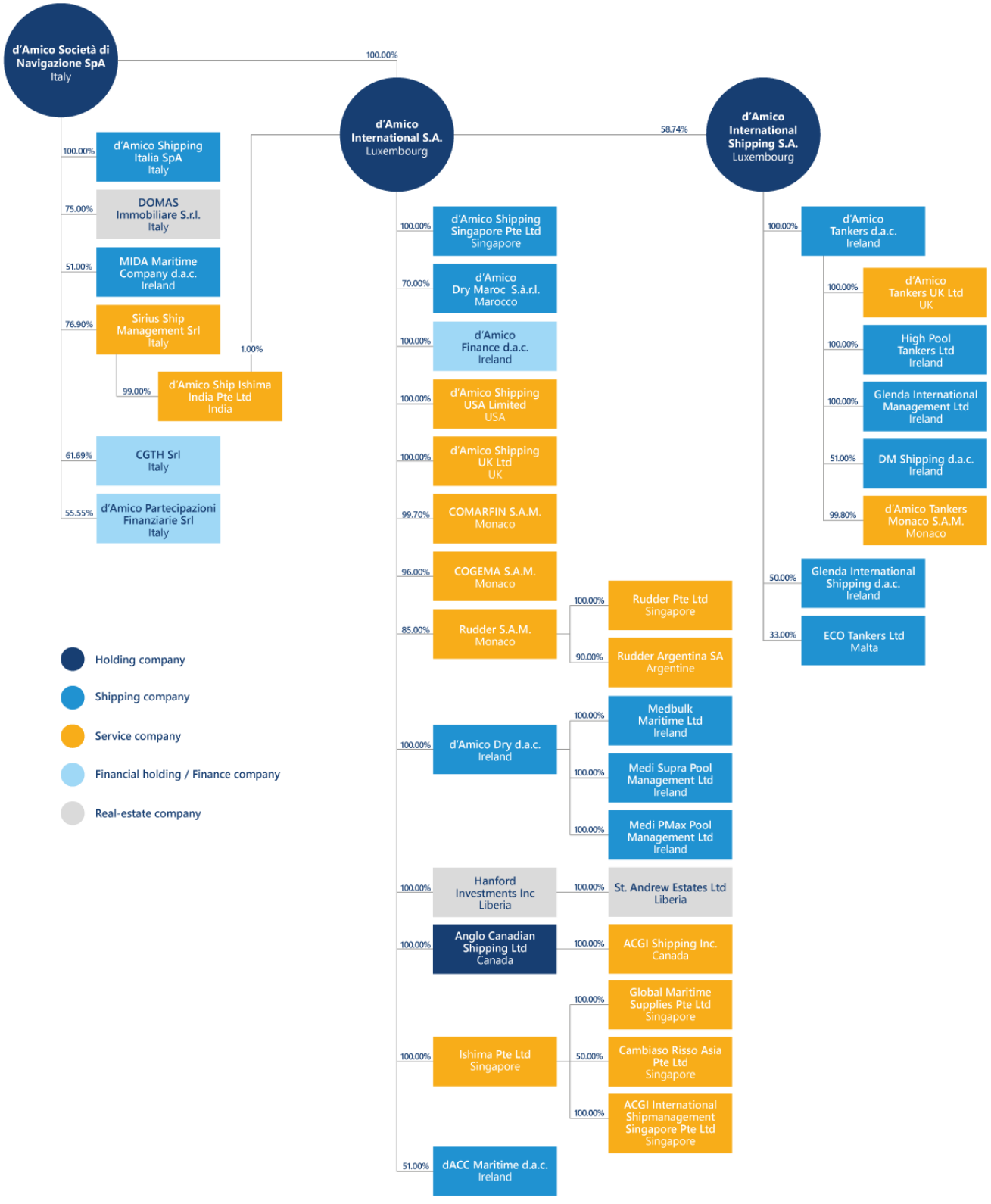
It is specified that the processing is carriying out both in paper and in electronic mode.

2. THE STRUCTURE AND CONTACT DETAILS OF THE GROUP

D'Amico Group is currently composed by 41 undertakings, operative in the following countries:

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

According to the following investments' structure:


d'Amico Società di Navigazione SpA
Italy
100.00%
d'Amico International S.A.
Luxembourg
58.74%
d'Amico International Shipping S.A.
Luxembourg
100.00% d'Amico Shipping Italia SpA Italy
75.00% DOMAS Immobiliare S.r.l. Italy
51.00% MIDA Maritime Company d.a.c. Ireland
76.90% Sirius Ship Management Srl Italy
99.00% d'Amico Ship Ishima India Pte Ltd India
1.00%
61.69% CGTH Srl Italy
55.55% d'Amico Partecipazioni Finanziarie Srl Italy
100.00% d'Amico Shipping Singapore Pte Ltd Singapore
70.00% d'Amico Dry Maroc S.à.r.l. Marocco
100.00% d'Amico Finance d.a.c. Ireland
100.00% d'Amico Shipping USA Limited USA
100.00% d'Amico Shipping UK Ltd UK
99.70% COMARFIN S.A.M. Monaco
96.00% COGEMA S.A.M. Monaco
85.00% Rudder S.A.M. Monaco
100.00% Rudder Pte Ltd Singapore
90.00% Rudder Argentina SA Argentine
100.00% d'Amico Dry d.a.c. Ireland
100.00% Medbulk Maritime Ltd Ireland
100.00% Medi Supra Pool Management Ltd Ireland
100.00% Medi PMax Pool Management Ltd Ireland
100.00% Hanford Investments Inc Liberia
100.00% St. Andrew Estates Ltd Liberia
100.00% Anglo Canadian Shipping Ltd Canada
100.00% ACGI Shipping Inc. Canada
100.00% Ishima Pte Ltd Singapore
100.00% Global Maritime Supplies Pte Ltd Singapore
50.00% Cambiaso Risso Asia Pte Ltd Singapore
100.00% ACGI International Shipmanagement Singapore Pte Ltd Singapore
51.00% dACC Maritime d.a.c. Ireland
100.00% d'Amico Tankers d.a.c. Ireland
100.00% d'Amico Tankers UK Ltd UK
100.00% High Pool Tankers Ltd Ireland
100.00% Glenda International Management Ltd Ireland
51.00% DM Shipping d.a.c. Ireland
99.80% d'Amico Tankers Monaco S.A.M. Monaco
50.00% Glenda International Shipping d.a.c. Ireland
33.00% ECO Tankers Ltd Malta
Holding company
Shipping company
Service company
Financial holding / Finance company
Real-estate company
as of 30 June 2017

The d'Amico Group, founded in 1952, is a world leader in maritime transportation in the Dry Cargo and Product Tankers sectors and offering international shipping services relating to the core businesses. It manages one of the largest fleets worldwide of product tankers, bulk and container vessels. With offices in over 10 maritime and financial centers worldwide, the d'Amico Group has over 350 ashore employees and over 3000 seafarers on board its vessels.[1]

Its mission and strategy have always been to respect and protect the environment, focus on customer care and the professional excellence of its own people.

The Head Quarter of the group is located in Rome.

Contact details:

Rome – Head Office

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

P +39 06 845 611

F +39 06 98968092

E info@damicoship.com

[1] Annual report of 31.12.2016

3. CATEGORIES OF DATA SUBJECTS/ PERSONAL DATA/ PROCESSING/ THIRD COUNTRIES WHERE DATA ARE TRANSFERRED TO

DSN, as part of the assessment activities for the development of the group privacy model, has identified the following categories of data subjects for which the transfer of data to countries outside European Union could be configured:

- Employees and Crew.
- Candidates
- Board Members

For each data subjects' categories, in the following tables are reported the following information:

- Types of data, which are subject to the processing: indicate the type of data processed for each category of data subject.
- Purposes of the processing: indicate the reasons or activities related to the specific processing of data.
- Legal basis of processing: indicates the legal basis of the processing, with particular reference to Art.6 "*lawfulness of processing*" of the Regulation.
- Modality of processing: indicates the name of the application (in the event that the storage is carried out electronically) or the name of the archive (in the event that the storage is carried out in paper mode) used for the management of the data relating to each category of data subjects.
- Third country which data are transferred to identifies, where applicable, the third country and/or the international organisation which personal data are trasnferred to.

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 diseasesi 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

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 controlled/linked companies 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.

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 2 - 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 controlled/linked companies, located in the following Non-EU countries: Principality of Monaco, Singapore, India, Morocco, USA and Liberia
External companies	n.a.

[2] 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.

Board Members

Categories of data	Purposes of the processing	Legal basis	Modalities	
			Electronic	Paper
Common personal data (personal data, education and culture, etc.)	*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.
Adiministrative and accounting data				

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 controlled/linked companies, located in the following Non-EU countries: Principality of Monaco, Singapore, India, Morocco, USA and Liberia
External companies	n.a.

References: General Data Protection Regulation 2016/679, 27 April 2016

4. THE LEGALLY BINDING NATURE OF THE "BCR" BOTH INTERNALLY AND EXTERNALLY

These rules are signed for unconditional acceptance by all the companies belonging to d'Amico group and are, therefore, legally binding both within the group and outside. Based on the contents of these rules, DSN carries out random audits on an annual basis at the offices of non-EU countries.

These audits are planned and managed by the group's Data Protection Officer on the basis of an annual audit plan, with the support of the Privacy Coordinators.

It will be given to the Company sufficient time to compensate for any deficiencies detected within the personal data management system referred to in these rules.

These rules are binding also for all the subjects that process data of the above mentioned data subjects as external data processors for the companies of the group outside the European Union (providers and professionals), for whom the acceptance of the same rules is expected in the context of commercial contracts.

References: General Data Protection Regulation 2016/679, 27 April 2016

5. GENERAL DATA PROTECTION PRINCIPLES

DSN and the Companies *in scope and out of scope* with the model have implemented the technical and organisational measures in order to ensure a proportionate level of security to the risks, which includes, among others:

- 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.

All in compliance with *privacy by design and privacy by default* principles, very important in the Privacy organisational model of d'Amico Group.

In particular, DSN, as the Holding of d'Amico Group, has carried out analyse and risk assessment activities, as required by the Regulation, an extract of which is reported in Annex 2.

References: General Data Protection Regulation 2016/679, 27 April 2016

6. THE RIGHTS OF DATA SUBJECTS AND THE PROTECTION OF PERSONAL DATA

DSN and the companies in *scope and out of scope* with the model have set up a privacy organisational system able to ensure the respect of data subjects' rights, as expected in Chapter III of the Regulation, called "*Rights of data subject*".

In particular, regarding to the categories of data subjects related to:

- Employees and Crew
- Candidates
- Board Members

DSN and the Companies *in scope and out of scope* with the model, provide information pursuant to Art. 13 of the Regulation, informing data subjects of the possible transfer of personal data concerning them to Group's controlled Companies, also outside the European Union and acquire their consent.

The information to be provided to data subjects contains all the elements provided for in the Regulation, including the rights of data subjects and the relating methods of operation.

In particular:

- right of access;
- right of rectification and erasure;
- right to restriction of processing;
- right to object.

These rights can be exercised by sending a request to the Group's Data Protection Officer by e-mail.

6.1. Third beneficiary clause

It is specified that, pursuant to these Binding Corporate Rules, the interested parties have the rights to assert the BCR against any d'Amico Group Company which has violated the BCR, by filing a complaint with the competent Supervisory Authorities, including the right of the parties concerned to obtain compensation for the damage related to the failure to comply with the provisions of these rules not only against the data Controller, but also against the external managers of the treatment or any sub-external

processors, if the direct recipient of the compensation request has disappeared or has legally ceased to exist.

7. RESPONSABILITY OF DSN AND COMPANIES IN SCOPE AND OUT OF SCOPE WITH THE MODEL, AS AUTONOMOUS CONTROLLERS

DSN and Companies *in scope and out of scope* with the model comply with the Regulation for what concern the controller's liability, consistently with Chapter IV, called "Controller and Processor".

In particular, DSN, as the Holding of the Group, has put into being a system of protection and guarantee of privacy and rights of data subjects, which is constantly updated, and which guarantees technical and organizational measures appropriate to the processings carried out.

The objective of the system is to ensure, by default, that only personal data necessary for the pursuit of specific purposes of the processing, both as regards to the amount of personal data collected, the scope of processing, and the retention period and accessibility.

The system finally ensures, by default, that personal data are not accessible to an undefinite number of natural persons without the intervention of the natural person.

For this purpose, DSN, as the Holding of d'Amico Group, has defined its own privacy organisation, structured as follows:

7.1. Data Controller **(Art.24)**

In quality of autonomous Data Controller, DSN, as the Holding of d'Amico Group, and Companies *in scope and out of scope* with the model, represent the main recipients of all the obligations provided by the Regulation; for this reason they 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).

7.2. Data Protection Officer (DPO) (art. 37)

According to art.37 of the Regulation, DSN, as the Holding of d'Amico Group, has designated a single Data Protection Officer, hereinafter DPO, as a member of the Data Controller of DSN, Miss Marzia Vona.

The appointment of 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 in HR office.

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

- should be involved, properly and in a timely manner, in all issues which relate to the protection of personal data; he should be provided with the resources necessary to carry out those tasks and, therefore, with a spending budget;
- should not be dismissed or penalised by the controller or the processor for performing his tasks;
- directly report to the highest management level of the controller or the processor;

- may be contact by data subject with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation;
- should 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 as long as they don't result in a conflict of interests.

The governance of the privacy management system through this figure will allow d'Amico Group, not only to compliance with the legal provisions on data protections, but also to control the legal responsibility profiles deriving from the application of the accountability principle.

The main tasks of the DPO are the following:

a) to coordinate and manage the Privacy Coordinators appointed by the data controller for each group location;
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.

7.3. Privacy coordinators (art.37)

DSN, as the Holding of d'Amico Group, in order to facilitate the coordination and management of actions aimed at compliance with the Regulations, has appointed a Privacy Coordinator for each country in the group at international level.

These figures are coordinated by the Group's DPO.

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

7.4. Data Processor (art. 28 and art. 29)

Pursant to art. 28 of the Regulation, "w*here 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 processors is therefore identified by the data controller among individuals who, for experience, ability and reliability, are able to provide a suitable guarantee of full compliance with the current provisions on processing, including the profile related to the security of personal data managed (both with the aid of IT tools and not).

Within d'Amico Group, the figure of the processor has been distinguished between:

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

7.4.1. Internal Data Processors

DSN and the companies *in scope and out of scope* with the model, that present a greater organizational complexity depending on the number of employees, as independent data controllers, have appointed as internal processors, the Heads of the Organizational Functions, who in the scope of their attributions, deal manually or with electronic means, personal data of which DSN and the companies *in scope* are Controllers. The appointments are formalized through a letter of appointment which regulates their duties in detail; a

copy of the appointment letters countersigned by the internal processors are filed at DSN's HR Dept. Organizational changes that may have an impact on the organization of internal processors must be communicated to the DPO, which assess and proposes to the Controllers any changes to be made to the organization.

7.4.2. External Data Processors

DSN and all the companies *in scope and out of scope* with the model are external data processors for the processing of data for the other companies of the group (each company is the external processor of the processing for all the others), regardless of the existing intra-group commercial contracts. This choice is motivated by the fact that it is not possible to exclude that, outside of the formalized commercial agreements, any transit of personal data relating to the data subjects may be configured.

All companies and professionals that provide services to the single companies of the group *in scope* with the model, which, in the assignment received, deal manually or with electronic means personal data of which DSN and the companies *in scope* are Controllers.

7.5. Persons in charge of the processing

DSN and the companies *in scope* with the model, as independent data controllers, have identified different classes of persons in charge of the processing, in which all the employees and collaborators of the various group's companies fall within the scope of their duties, dealing manually or with electronic tools, personal data of which DSN and the companies *in scope* are Controllers.

This appointment is formalized through a specific letter that governs its tasks; copies of the designation letters countersigned for inspection by the persons in charge are filed by the DPO at its office.

7.6. System Administrators

DSN and the companies *in scope* with the model, as autonomous Controllers, have appointed as System Administrators, the employees and collaborators with particular tasks and responsibilities in the management and maintenance of business applications and of the technological infrastructure, in accordance with the provision of point 2, let.c. of the Measures and arrangements referred to in par. 1.2 which states "*Information required to identify the natural persons working as system administrators including*

a list of the functions committed to them must be reported in an internal document that should be updated regularly and made available for inspection by the Italian DPA".

References: General Data Protection Regulation 2016/679, 27 April 2016

8. THE MODALITIES OF THE INFORMATION PROVIDED TO DATA SUBJECTS

Data subjects are informed about the existence of BCR in different ways according to the categories data subjects:

Data subjects	Communication modalities
Employees	Publication of the "Binding Corporate Rules" on the Corporate Intranet and internal communication to all staff by the HR Dept. on the publication of the rules, with links for viewing and / or saving the file locally.
Crew	Communication to all staff by the Crewing Dept. by email with attached BCR and links to the company Intranet. Communication through the onboard newsletter (Lighthouse).
Candidates	Publication of the abstract of the "Binding Corporate Rules" on the Internet site www.damicoship.com, within the reserved area for the submission of applications.
Board Members	Publication of the "Binding Corporate Rules" on the Corporate Intranet and internal communication to all staff by the HR Department on the publication of the rules, with links for viewing and / or saving the file locally. Sending by e-mail the "Binding Corporate Rules" to all members of Board Members that do not fall into the category of employees and collaborators.

9. DATA PROTECTION OFFICER (DPO)

According to art.37 of the Regulation, DSN, as the Holding of d'Amico Group, has appointed single Data Protection Officer (DPO) at corporate level, as a member of the Data Controller of DSN, Miss Marzia Vona

The appointment of the DPO is formalized through a customized letter on the basis of the processings performed, which regulate the tasks.

DPO:

- is involved, properly and in a timely manner, in all issues which relate to the protection of personal data; he should be provided with the resources necessary to carry out those tasks and, therefore, with a spending budget;
- cannot be dismissed or penalised by the controller or the processor for performing his tasks
- directly reports to the highest management level of the controller or the processor
- may be contact by data subject with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation
- is 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 as long as they don't result in a conflict of interests.

The governance of the privacy management system through this figure will allow the Controller, not only to compliance with the legal provisions on data protections, but also to control the legal responsibility profiles deriving from the application of the accountability principle.

The main tasks of the DPO are the following:

g) to coordinate and manage the Privacy Coordinators appointed by the data controller for each group location;

References: General Data Protection Regulation 2016/679, 27 April 2016

h) 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;

i) 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;

j) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;

k) to cooperate with the supervisory authority;

l) 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.

References: General Data Protection Regulation 2016/679, 27 April 2016

10. COMPLAINT PROCEDURES

DSN has set up a complaint procedure by the data subjects that applies to all the companies of the group, which provides for the filing of a form to be sent to the attention of the DPO. This form can be sent by e-mail or through the local privacy coordinators.

The fields of the form must be filled in in detail in order to allow the DPO to carry out the investigations necessary to assess the complaint and to propose any corrective actions to DSN.

The form is available on the web site http://www.damicoship.com.

References: General Data Protection Regulation 2016/679, 27 April 2016

11. THE MECHANISMS WITHIN THE GROUP OF UNDERTAKINGS, FOR ENSURING THE VERIFICATION OF COMPLIANCE WITH THE BINDING CORPORATE RULES.

The mechanisms put in place by DSN, as the Holding of the d'Amico group, for ensuring the verification of compliance with BCR, including data protection audits and methods for ensuring corrective actions to protect the rights of the data subjects in the controlled undertakings, is described below:

- Risk Assessment.
- Privacy Impact Assessment - PIA
- Organizational procedures.

Results of such verification are communicated by the DPO to the administrative body of the subsidiaries of DSN and made available, on request, to the competent Supervisory Authority.

References: General Data Protection Regulation 2016/679, 27 April 2016

12. THE MECHANISMS FOR REPORTING AND RECORDING CHANGES TO THE RULES AND REPORTING THOSE CHANGES TO THE SUPERVISORY AUTHORITY

In order to ensure the constant updating to the Supervisory Authorities of any changes made to these Rules, DSN, as the holding company of the d'Amico group, will follow the procedures provided for by the legislation, with particular reference to CHAPTER V "*Transfers of personal data to third countries or international organizations* ".

References: General Data Protection Regulation 2016/679, 27 April 2016

13. COOPERATION WITH SUPERVISORY AUTHORITY

DSN, as the holding of the d'Amico group, collaborates and cooperates with the competent Supervisory Authorities, providing all the necessary support in case of information needs, in-depth analysis and reports.

The designated DPO is the point of contact with the competent Authorities, and ensures timeliness of response in case of requests from these Authorities.

References: General Data Protection Regulation 2016/679, 27 April 2016

14. THE MECHANISMS FOR REPORTING TO THE COMPETENT SUPERVISORY AUTHORITY

DSN, as the holding of d'Amico group, constantly reports, through the designated DPO, any legal requirements to which a member of the group of undertakings is subject in a third country which are likely to have a substantial adverse effect on the binding corporate rules, immediately highlighting the relevant elements and any need for updating them.

References: General Data Protection Regulation 2016/679, 27 April 2016

15. THE TRAINING TO PERSONNEL ON DATA PROTECTION

In order to ensure compliance with EU Regulation 2016/679, DSN and the companies *in scope* with the model, plan training sessions, with the aim of developing skills and abilities in the field of personal data protection.

In particular, the sessions are planned by the DPO with the support of the Privacy Coordinators and foresee the following minimum training sessions on an annual basis:

- training for persons in charge of the processing
- training for internal processors

In addition to the planned annual sessions, the DPO, with the support of the Privacy Coordinators, organizes special training sessions on the occasion of significant organizational and / or regulatory changes and training sessions dedicated to the Crew.

16. ANNEX TO BCR

References: General Data Protection Regulation 2016/679, 27 April 2016

ANNEX 1 THE PRIVACY MODEL OF THE GROUP

This document consists in n.2 sections:

- Section I - *Executive Summary*, which describes the objectives, the activities carried out and the group privacy model as defined at the outcome of the assessment activities.
- Section II - *Performed activities*, which describe the detailed activities carried out for the definition of the group model.

References: General Data Protection Regulation 2016/679, 27 April 2016

SECTION I - EXECUTIVE SUMMARY

1.1 PREMISES AND OBJECTIVES

The d'Amico Group, founded in 1952, is a world leader in maritime transportation in the Dry Cargo and Product Tankers sectors and offering international shipping services relating to the core businesses.

It manages one of the largest fleets worldwide of product tankers, bulk and container vessels. With offices in over 10 maritime and financial centers worldwide, the d'Amico Group has over 350 ashore employees and over 3000 seafarers on board its vessels.

Its mission and strategy have always been to respect and protect the environment, focus on customer care and the professional excellence of its own people.

D'Amico Societa di Navigazione S.p.A., hereinafter DSN, as the Holding of d'Amico group, has set out, starting from 2015, a self-assessment of its organization in the privacy field and a privacy assessment in its companies with the following objectives:

- Detect, verify and assess the correct application of privacy legislation;
- Assess the feasibility of the privacy model for the entire business group.

This choice, driven by the need to define corporate governance of privacy matters, in order to ensure the respect of the rights of data subjects in all the companies of the d'Amico group, was carried on in the following years, due to the opportunity provided from Regulation n. 679/2016 on the "*protection of natural persons with regard to the processing of personal data, as well as on the free movement of such data and repealing Directive 95/46 / EC (General Data Protection Regulation*)", hereinafter Regulation, which introduced the concept of "group of undertakings"[3].

[3]«Group of undertakings»: means a controlling undertaking and its controlled undertakings. See *Art. 4 "Definitions", point 19) of the EU Regulation 2016/679.*

1.2 SUMMARY OF THE ACTIVITIES CARRIED OUT

The assessment activities were conducted through the analysis of the following documents:

- EU Regulation 2016/679
- D'Amico Organization Chart as of 31 August 2016 - WIP
- D'Amico Organization Chart as of 30th June 2016 – FINAL
- Structure of the Group as of 30th June 2016 and 30th June 2017
- Consolidated Financial Statements as of 31th December 2015 and 31th December 2016 of DSN and DIS S.A.
- PRV-01 Register of the persons in charge of processing
- PRV-DPS_Rev8_DSN_DSH_2013_v1_SF_RA
- P-207 Data Protection_rev.2.01
- P-207 Annex 1 Data Protection_rev.2.01
- Documents related to the privacy system in place in DSN (for example, internal and external processors, designation persons in charge of processing and System administrators, privacy information)
- Documents related to the privacy system in place at the following controlled companies: d'Amico International S.A (Luxembourg), Cogema S.A.M. (Principality of Monaco), d'Amico Shipping UK Ltd (United Kingdom), ISHIMA Pte Ltd (Singapore), d'Amico Shipping USA Limited (Stamford, USA) and d'Amico Dry d.a.c. (Ireland) (for example internal and external processors' appointments, designation of persons in charge of processing and System administrators, privacy information).

It is specified that the choice to carry out the assessment on these companies was driven by their representativeness at Corporate level.

The assessment for the controlled undertakings was conducted through the administration of a check list and interviews with local privacy contacts.

Following the assessment of the controlled companies, a summary report of the activities was produced, with details of the results for each legal entity.

1.3 RESULTS

The assessment activities have outlined a framework of substantial compliance with the requirements established in the field of privacy at the level of local regulations by the companies subject to verification.

However, in order to ensure a role of direction, monitoring and control by DSN on its subsidiaries in privacy matters, a group privacy model has been developed, according to which DSN and its controlled undertakings act as independent data controllers, with a guide by DSN regarding the policies to be followed within the group for the correct application of privacy legislation.

The "Section II" of this document contains the detailed activities and the rationals that led to the definition of the group privacy model.

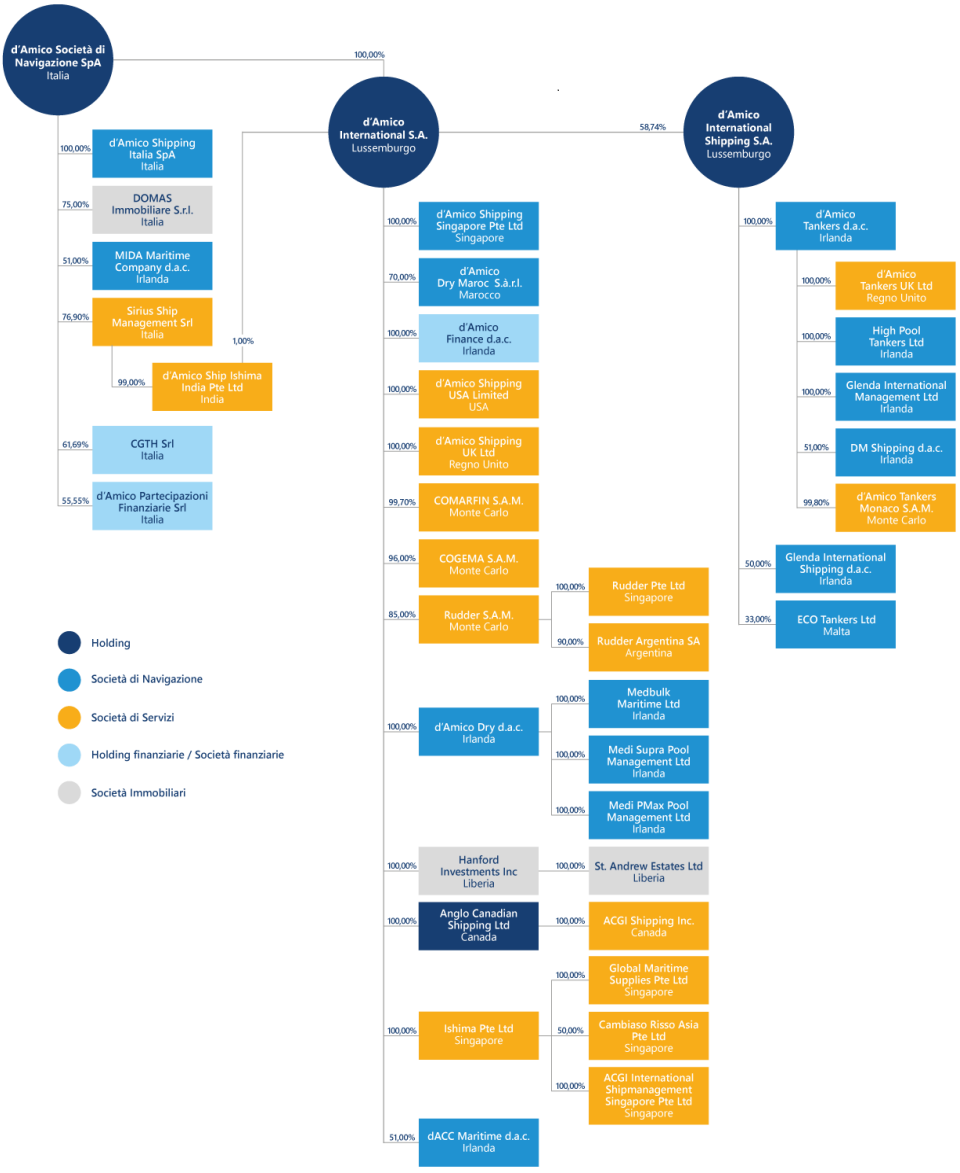
References: General Data Protection Regulation 2016/679, 27 April 2016

SECTION II – PERFORMED ACTIVITIES

2.1 D'AMICO GROUP PRIVACY MODEL

2.1.1 The structure

The structure of d'Amico group privacy model as of 30th June 2017 is reported below:



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[4].	Luxembourg	Holding
8	d'Amico International Shipping S.A.	Luxembourg	Holding
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

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

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

2.1.2 Categories of data subjects

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

- Employees and Crew[5];
- Candidates;

[5] This category refers to all employees of the Company.

- Customers and Prospect;
- Suppliers [6];
- 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.

[6] External Professionals are included in this category.

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.

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.

2.1.3 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[7], 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).

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

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 subsidiaries.

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

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
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

2.1.4 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:

- Data Controllers: DSN and all the controlled companies *in scope* with the model are autonomous Controllers for the categories of data subjects reported in paragraph 1.2. "The categories of data subjects of d'Amico group".

  As already explained above, for these companies DSN exercises the role of direction, monitoring and control, as the Holding, for the correct application of the rules for the management of privacy defined at Corporate level.

- Internal Data Processors: DSN and the companies *in scope* with the model that have a greater organizational complexity depending on the number of employees, as

independent data controllers, have appointed as Internal Data processors, the Heads of the Functions Organizations, which in the context of their duties, process manually or electronically, personal data of which DSN and the companies *in scope* are Controllers.

- Persons in charge of processing: DSN and the companies *in scope* with the model, as autonomous data controllers, have identified different Classes of persons in charge in which all the employees and collaborators of the various Group companies, falling within the scope of their duties, deal manually or with electronic means, personal data of which DSN and the companies *in scope* are Controllers.
- External Data Processors:

  DSN and all the companies *in scope and out of scope* with the model are External Processors of data for the other companies of the group (each company is the external data processor for all the others), regardless of the existing intra-group commercial contracts. This choice is motivated by the fact that it is not possible to exclude that, outside of the formalized commercial agreements; any transit of personal data relating to data subjects may be configured.

  All companies and professionals that provide services to the single companies of the group *in scope* with the model, which in their tasks, deal manually or with electronic means, personal data of which DSN and the companies *in scope* are Controllers.
- Data Protection Officer (DPO): in compliance with art. 37 of the Regulations, DSN has designated as Data Protection Officer at Corporate level, in staff of the Controller of DSN, Miss Marzia Vona.
- Privacy Coordinators: DSN, in order to facilitate the coordination and management of actions aimed at compliance with the Regulations, has appointed a Privacy Coordinator for each country in the group at international level.

References: General Data Protection Regulation 2016/679, 27 April 2016

ANNEX 2 RISK ASSESSMENT

1. Risk assessment (art.32)

Risk analysis refers to 2018 for the 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.

To complete the scenario, it is important to specify 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.

2. 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.

2.1. 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:

2.1.1 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.

2.1.2 *Identification of harmful events a 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.

2.1.3 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.).

2.1.4 Detection of the 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.

2.2. 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

2.2.1 Determination of the inherent risk level

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.

References: General Data Protection Regulation 2016/679, 27 April 2016

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: General Data Protection Regulation 2016/679, 27 April 2016

2.2.2 *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

2.2.3 *Identification and assessment of the options for treating risk*

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.

2.3. Assessment results

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

2.3.1. Risk identification

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.

2.3.1.1. 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.

References: General Data Protection Regulation 2016/679, 27 April 2016

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.

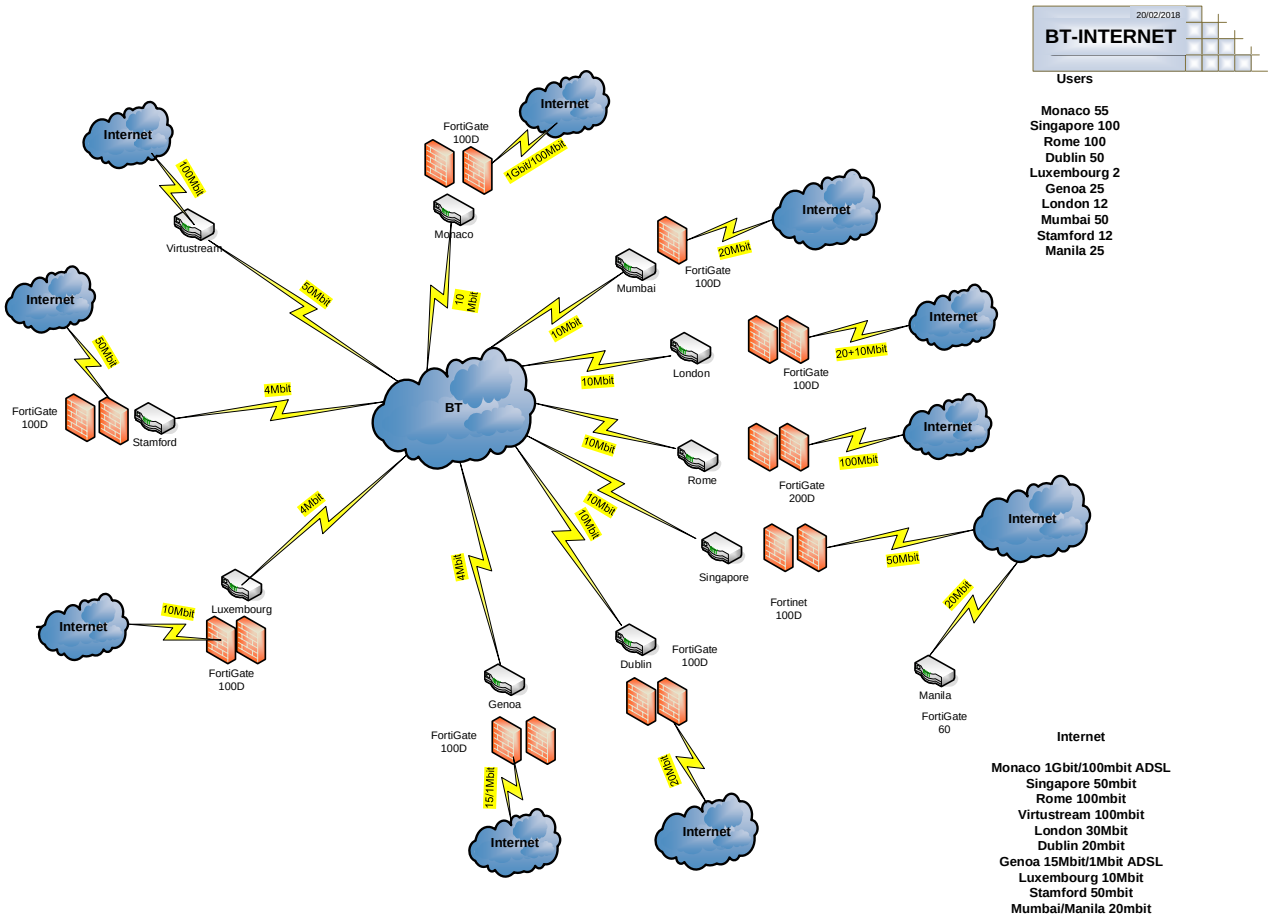
The workstations located at d'Amico offices are connected to the company LAN, allowing the use of network units with limited access to the personnel belonging to the Company Departments, network units with access restricted to individual employees and network units for document exchange.

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.

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

References: General Data Protection Regulation 2016/679, 27 April 2016

Figure 1 –d'Amico Group's technological infrastructure



Applications and the related database in d'Amico, which fall within the scope of the Regulation are detailed in "*DAMICO ICT Infrastructure and Applications*"

2.3.1.2. 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.

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

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	Adequate	Low

Context	Event	Risk factors	Impact	Likelihood	Inherent risk	Protection measures in place	Control assessment	Residual risk
						- Adoption of strong authentication rules ITG-09 Users Accounts - 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

Context	Event	Risk factors	Impact	Likelihood	Inherent risk	Protection measures in place	Control assessment	Residual risk
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 which the applications and data reside - Contract Cloud Providers	Adequate	Low
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	M	L	L	- ITG-09 Users Accounts - WI-ITG-04 Users Authorization register - Monitoring of failed access attempts	Adequate	Low

Context	Event	Risk factors	Impact	Likelihood	Inherent risk	Protection measures in place	Control assessment	Residual risk
		position held - Absence of an access control policy						
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

Context	Event	Risk factors	Impact	Likelihood	Inherent risk	Protection measures in place	Control assessment	Residual risk
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 - ITG-11 IS Configurations	Adequate	Low
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

Context	Event	Risk factors	Impact	Likelihood	Inherent risk	Protection measures in place	Control assessment	Residual risk
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 - Quarterly Risk Report - Weekly Network Threats Report - Half Year Administrator Log Report - Bridge and NAV Network Security - Risk Assessment - Ethical hackers campaign	Adequate	Medium
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

Context	Event	Risk factors	Impact	Likelihood	Inherent risk	Protection measures in place	Control assessment	Residual risk
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
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

2.5. Final Considerations

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

2.6. 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