Contents

1. Overview of GDPR

The General Data Protection Regulation (Regulation (EU) 2016/679-hereinafter "GDPR") is a regulation by which the European Union intends to strengthen and unify data protection for all individuals within the European Union (EU).

2. Definitions

Biometric Data - personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopy data

Company – SAMOS STEAMSHIP Co legal entity

Consent [of the data subject] 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;

Data Concerning Health - 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;

Data Controller - 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.

Data Portability- the requirement for controllers to provide the data subject with a copy of his or her data in a format that allows for easy use with another controller.

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

Data Protection Coordinator (DPC)- an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR.

Data Protection Team (hereinafter DP Team or DPT)- a team which is responsible for compliance of the Company with GDPR

Data Subject- a natural person whose personal data is processed by a controller and/or processor

Encrypted Data- personal data that is protected through technological measures to ensure that the data is only accessible/readable by those with specified access

Encryption key- is typically a random string of bits generated specifically to scramble and unscramble data

The **European Economic Area (the EEA)** consists of the EU Member States together with Iceland, Liechtenstein and Norway. Any other country or territory is considered to be a 'third country' for the purposes of the GDPR.

Genetic Data- 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

Personal Data - 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.

Personal Data Breach - 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.

Privacy by Design - a principle that calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition.

Privacy Impact Assessment– a methodological tool used to identify and reduce the privacy risks of entities by analysing the personal data that are processed and the policies in place to protect the data.

Processing- 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.

Profiling- 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.

Recipient- 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 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.

Regulation- a binding EU legislative act that must be applied in its entirety across the Union

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

Special Category Data - More sensitive information relating to an individual's race/ethnic origin, political opinions/affiliations, religious beliefs, trade union membership, health related, sexual life and biometrics.

3. Introduction

This Privacy Policy applies to the **SAMOS STEAMSHIP CO,** 63 Poseidonos Ave. & 2 Aiantos str., P. Faliro 175 62, Athens, Greece, (hereinafter collectively "SAMOS STEAMSHIP").

SAMOS STEAMSHIP is committed to compliance with the European Union General Data Protection Regulation (hereinafter referred to as "GDPR") and the national legislation as in force (Law No. 4624/2019). Non-compliance may expose SAMOS STEAMSHIP to complaints, regulatory action, fines and/or reputational damage.

This policy describes how personal data is collected, handled, and stored to meet the company's lawful data protection standard.

4. Scope

The purpose of a privacy policy to set out the conditions under which SAMOS STEAMSHIP processes personal data in its capacity as data controller, including the special categories of personal data and to ensure that everyone in the business is aware of their individual responsibilities and the SAMOS STEAMSHIP' s data protection standards.

That may include any information (including opinions and intentions) which relates to an identified or identifiable natural person.

SAMOS STEAMSHIP may receive such information from other individuals that it has a business relationship with or with whom it may need to enter into a contract, involving among others, employees, crew members, managers and directors; current, prospective and former clients, business partners, suppliers, brokers, charterers, agents, advisers, external consultants and experts, inspectors and surveyors, third parties onboard vessels and representatives of all the above visitors and job applicants.

This policy supplements all other policies relating to internet and email use. SAMOS STEAMSHIP may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy related to data protection is circulated to staff before being adopted.

5. Policy Goals

This Policy ensures that SAMOS STEAMSHIP:

- Complies with General Data Protection Regulation EU 2016/679 (“GDPR”) and the national legislation as in force.
- Protects the rights of data subjects.
- Recognizes the need to share data with other organisations.
- Ensures that adequate procedures and protections are in place to lawfully fulfill and meet all of these requirements;
- Protects itself from the risks of data breach.

6. General Staff Guidelines

- The only personnel allowed to access data covered by this policy are those who need it for professional and lawful reasons.
- Employees must keep all data secure, by taking sensible precautions and following the guidelines in accordance with the office security and cyber security policy, as applicable.
- In particular, passwords must be used, based on SAMOS STEAMSHIP corresponding procedures.
- Personal data must not be disclosed to unauthorised individuals, either within the company or without.
- The company provides training to all employees to raise awareness and understanding about their responsibilities when handling data.
- Personal Data shall be regularly reviewed and updated if and to the extent they are determined to be out of date. If no longer required, such data are to be deleted and destroyed.

7. Company's Principles (GDPR Art. 5)

SAMOS STEAMSHIP has adopted the following principles to govern its collection, use, retention, transfer, disclosure and destruction of personal data:

7.1 Lawful (GDPR Art. 6), Transparent and Fair Processing (GDPR Art. 12)

SAMOS STEAMSHIP processes personal data fairly, lawfully and in a transparent manner in accordance with data subjects' rights.

This means, SAMOS STEAMSHIP:

- informs data subjects about what processing will be carried out (transparency),
- ensures the processing matches the description given to the data subject (fairness),
- requires the processing to be one of the purposes specified in the applicable GDPR regulation (lawfulness).

7.2 Data Purpose Specification

SAMOS STEAMSHIP adequately processes accurate personal data obtained for a specific purpose unless:

- the individual concerned has explicitly agreed to this or
- based on the individual's relationship with SAMOS STEAMSHIP, further processing meets the reasonable expectations of data subject.

7.3 Data Security

SAMOS STEAMSHIP safeguards personal data against loss or misuse.
In case of data processing assignment to third parties, SAMOS STEAMSHIP establishes whether additional data security arrangements need to be provided for.

7.4 Data Storage

- Personal data relating to SAMOS STEAMSHIP are stored only on SAMOS STEAMSHIP's approved devices and in a secure way.
- In cases where data are stored on paper, they are kept in a physically secure place where unauthorised personnel cannot access it.

- Printed data are shredded when they are no longer needed.
- Data stored on a computer are protected by strong passwords that are changed regularly according to SAMOS STEAMSHIP Password policy.
- Data stored on CDs or memory sticks, are removed securely when they are not being used.
- SAMOS STEAMSHIP ensures cloud provider's compliance with GDPR by way of signing appropriate data processing agreements.
- Data are regularly backed up in line with the company's back-up procedures.
- All servers containing Personal Data are properly protected by security tools.

7.5 Data Processing

SAMOS STEAMSHIP processes personal data of its contacts for the following purposes:

- The general administration and business administration of SAMOS STEAMSHIP.
- To comply with obligations imposed by laws or regulations.
- Based on Contracts.
- To serve SAMOS STEAMSHIP legitimate interests, to the extent that such interests are not overridden by the interests or fundamental rights and freedoms of data subjects.

The following general principles apply:

- When working with personal data, employees ensure the screens of their computers are always locked when left unattended.
- Personal data are not to be shared informally.
- Data, if necessary, will be encrypted before being transferred electronically.
- Personal data are transferred outside EU according to the data transfer mechanisms that SAMOS STEAMSHIP has developed.

7.6 Data Accuracy

- SAMOS STEAMSHIP ensures data are accurate and up to date.
- Data subjects can update information provided to SAMOS STEAMSHIP by sending a request to: gdpr@samossteamship.gr.

8. Data Mapping

To comply with the GDPR, SAMOS STEAMSHIP as a first step identifies and locates personal data , and continues to do so regularly, in its systems and outlined to what processing such personal data is subject. The data mapping tool, among others, demonstrates a transfer of information from one location to another.

Data Mapping Procedure

Data mapping required comprehensive information gathering from all business units, and visualisation of the information gathered. Critical to this action, was the capturing of details on the categories of personal data, data subjects, purposes of processing, the destination of data, accessing etc.

SAMOS STEAMSHIP used and continues to use a structured and planned data mapping approach which includes the following steps:

(a) **Appoint a person/ team responsible for creating and maintaining the data map.** This team is comprised of individuals from various business units involved in data processing activities.

(b) **Define a project plan.** The data mapping team creates a project plan which outlines the project scope and level of detail as well as the necessary activities, timelines and responsibilities.

(c) **Gather relevant information.** The data mapping team interviews and surveys individuals involved in the in-scope data processing activities, review IT processes and consult potentially existing (partial) data maps and other documents.

(d) **Prepare the data map based on the gathered information.** The data mapping team addresses any inefficiencies and gaps in the data flow that the data map might reveal.

(e) **Maintain and update the data mapping document.** Once prepared, the data mapping document needs to be regularly updated to stay relevant.

9. Data Collection

Data Sources: Personal data are collected from a data subject if one of the following conditions applies:

- The nature of the business purpose necessitates collection of the personal data.
- The collection is carried out under emergency circumstances in order to protect the vital interests of the data subject or to prevent serious loss or injury to another person.

Where it has been determined that notification to a data subject is required, privacy notice is given promptly.

Where a need exists to request and receive the consent (as described below) of an individual prior to the collection, use or disclosure of their personal data, SAMOS STEAMSHIP is committed to seeking such consent.

9.1 Data Subject Consent (GDPR Art. 7)

In certain cases, SAMOS STEAMSHIP may collect personal data under the data subject's consent.
The data subject retains the right to revoke this consent at any time.

9.1.1. Conditions for consent

- Keeping records to demonstrate consent;
- Consent is specific and informed: prominence and clarity of consent requests, the consent covers the controller's identity and the purposes of processing;
- Unambiguous indication: obvious that the individual has clearly consented, and what they have consented to;
- The right to withdraw consent easily and at any time; and
- Freely given consent if a contract is conditional on consent.

9.1.2 Principles for Consent

SAMOS STEAMSHIP processes personal data in accordance with all applicable laws and applicable contractual obligations.

The DP team/DP Coordinator, in cooperation with the Legal Advisor and IT department, and other relevant business representatives, establishes a system for obtaining and documenting data subject consent for the collection, processing, and/or transferring of their personal data.

The system includes provisions for:

- Determining what disclosures are made in order to obtain valid consent.
- Ensuring the request for consent is presented in a manner which:
    a. Is clearly distinguishable from any other matters,
    b. is made in an intelligible and easily accessible form,
    c. uses clear and plain language.
- Ensuring the consent is freely given.
- Documenting:
    a. the date, method and content of the disclosures made,
    b. the validity, scope, and will of the consents given.
- Providing a simple method for a data subject to withdraw their consent at any time.

Consent can be given only in writing form.
The consent form is sent to the data subject by SAMOS STEAMSHIP either by fax, post or e-mail.
In other cases SAMOS STEAMSHIP may obtain consent through the following active opt-in mechanisms:

- signing a consent statement on a paper form;
- ticking an opt-in box on paper or electronically;
- clicking an opt-in button or link online;
- selecting from equally prominent yes/no options;
- choosing technical settings or preference dashboard settings;
- responding to an email requesting consent.

The consent form, at a minimum, includes the following:

- The name of the organisation and the names of any third parties who will rely on the consent;
- Why SAMOS STEAMSHIP needs the data;
- How SAMOS STEAMSHIP will process the data;
- The right of individuals to withdraw their consent at any time.

9.1.3. Record of consent

Record keeping of consent forms must be maintained by SAMOS STEAMSHIP.

Review of consents' status:
DP team/DP Coordinator reviews the status of data subject's consents every year, assuring the stability of relationship, the data processing and its purposes.

9.1.4. Withdrawals of consent

Data subjects are able to give and withdraw their consent in the same manner at any time.

SAMOS STEAMSHIP responds immediately when a request for withdrawal of consent is received.

9.2 Data Processing

Conditions for Processing

SAMOS STEAMSHIP does not process personal data unless it has identified a lawful basis for the processing, i.e. provided that at least one of the following requirements are met:

- 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;
- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary in order to protect the vital interests of the Data Subject or of another natural person;
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of Personal Data, in particular where the data subject is a child.

SAMOS STEAMSHIP ensures any use of personal data is justified using at least one of the conditions for processing, and this is specifically documented.

SAMOS STEAMSHIP provides 'privacy notices' to deliver explanations to individuals when information is collected about them.

Privacy Notice Form must be:

- in a clear, written and straightforward language;
- easily understood;
- aligned with organisation's values and principles;
- truthful and honest.
- consistent and can be updated easily.
- given free of charge.

SAMOS STEAMSHIP may provide privacy notices through a variety of forms:

- In writing - printed media; forms, such as job application forms or agreements, such as employee agreements.
- Electronically - in text messages; on websites; in emails; on mobile apps.

SAMOS STEAMSHIP delivers privacy notices, in the same manner it uses to collect personal data.

When SAMOS STEAMSHIP is collecting information through an online form, the privacy notice is provided as the individual fills out the form.

SAMOS STEAMSHIP, among other, provides the following information through the privacy notices:

a. identity and contact details of SAMOS STEAMSHIP;
b. the contact details of the data protection coordinator;
c. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
d. the legitimate interests, where processing is necessary for the purposes of the legitimate interests pursued by SAMOS STEAMSHIP or by a third party;
e. the recipients or categories of recipients of the personal data, if any;
f. the fact that SAMOS STEAMSHIP intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.
g. the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

h. the existence of the right to request from SAMOS STEAMSHIP access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
i. the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
j. the right to lodge a complaint with a supervisory authority;
k. whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
l. the existence of automated decision-making, including profiling, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Privacy notices for wide range of individuals

SAMOS STEAMSHIP is dealing with a wide range of individuals such as employees, candidates, crew members, suppliers, service providers, manning agents, etc. so privacy notices are provided in a separate way to different categories of individuals.

SAMOS STEAMSHIP regularly reviews the privacy notice, to:

- ensure that it remains accurate and up to date;
- analyze complaints from the public about how SAMOS STEAMSHIP uses their information and any claims about how SAMOS STEAMSHIP explains the use of their data;
- update privacy notice to reflect any new or amended processing.

9.3 Special categories of data

SAMOS STEAMSHIP processes special categories of data (also known as sensitive data) to comply with employment, legal or statutory obligations and respond to or defend any claim, and in specific and limited circumstances i.e. if requested by authorities for safety and security reasons.

In relation to health data of employees or crew members which are processed and may be transferred are only for social security arrangements, to liability insurers, health facilities and entities, in order to assist with medical treatment and insurance claims.

10. Data Retention

SAMOS STEAMSHIP retains personal data for no longer than necessary and for the purposes for which the data are collected or processed.
SAMOS STEAMSHIP's obligation regarding data retention arises from local laws or regulations or from contracts with employees, external third parties, charterers, or other providers.

- Data are retained in order to protect SAMOS STEAMSHIP's interests, preserve evidence, and generally conform to good business practices and for reasons such as stated here below but not limit to litigation;
- Accident investigation;
- Security incident investigation;
- Regulatory and statutory requirements.

The record retention schedule is as follows:

Record Type	Retention Period
Accounting and Finance	20 years
Contracts	20 years
Corporate records (minutes of the Board, bylaws, annual corporate reports)	20 years
Electronic mail	20 years
Insurance records	20 years
Legal files and papers	Termination + 20 years
Payroll documents	Termination + 20 years
Personnel & Crew records	Termination + 20 years
Tax records	20 years

Unless otherwise specified by relevant legislation.

When the retention period is over, SAMOS STEAMSHIP destroys the respective documents.

SAMOS STEAMSHIP implements procedures to govern the destruction of personal information. The manager of each department is responsible for enforcing the retention, archiving and destruction of documents and communicating the confirmation to the DPC.

Physical or technical destruction is defined as sufficient, when the information contained in the document becomes irretrievable. To this effect, relevant confirmation will be sent to the DPC once the process has been completed. At the time of destruction, shredding or other methods to be used so the information is completely destroyed.

In the case of data stored digitally, adequate methods include overwriting the content or demagnetizing, depending on the case.

All copies and duplicates should also be destroyed.

Exceptions to all the above, are requested by the head of the department and approved by the Company's Legal Advisor or any other department SAMOS STEAMSHIP thinks appropriate.

If any information retained under this policy is stored in an encrypted format, SAMOS STEAMSHIP takes appropriate measures to secure storage of the encryption keys.

11. Data Protection

SAMOS STEAMSHIP adopts physical, technical, and organisational measures to ensure the security of personal data. This includes the prevention of loss or damage, unauthorised alteration, access or processing, and other risks to which it is exposed by virtue of human action or the physical or natural environment.

Data Protection principles apply to all employees and third parties, for all information and any system used.

The procedures described in this policy must be followed at all times by SAMOS STEAMSHIP's employees, agents, contractors, or other third parties working for or acting on behalf of SAMOS STEAMSHIP.

12. Policies and Procedures

The procedures are to be added by SAMOS STEAMSHIP in line with the updated Cyber Security Manual and Office Security Manual.

13. Personal data Protection

SAMOS STEAMSHIP adopts physical, technical, and organisational measures to ensure the security of personal data. This includes the prevention of loss or damage, unauthorised alteration, access or processing, and other risks to which it is exposed by virtue of human action or the physical or natural environment.

The minimum set of security measures which has been adopted by SAMOS STEAMSHIP is provided in the present Policy. A summary of the personal data related security measures is provided below:

- Prevent unauthorised persons from gaining access to data processing systems in which personal data are processed.
- Prevent individuals entitled to use a data processing system from accessing personal data beyond their needs and authorisations.
- Ensure that personal data in the course of electronic transmission during transport cannot be read, copied, modified or removed without authorisation.
- Ensure that access logs are in place to establish whether, and by whom, the personal data was entered into, modified on or removed from a data processing system.
- Ensure that in the case where processing is carried out by a data processor, the data can be processed only in accordance with the instructions of the data controller.
- Ensure that personal data is protected against undesired destruction or loss.
- Ensure that personal data collected for different purposes can and is processed separately.
- Ensure that personal data is not kept longer than necessary.

14. Log Files Monitoring

Use Log files as historical records of the running state of hardware and software, storing information on how they are used, errors that occur and application specific events which

detail how users interact with them. Unauthorized users are not permitted to modify or interrupt the processes that are used to create log files on devices.

Log data generated are described in the Cyber Security Manual and also include the following source classes:

- Services that provide functionality to users
- Infrastructure supporting the network
- Host devices
- Remote connection services

15. Third Party Management

SAMOS STEAMSHIP in order to operate at the highest level of standards may request a Third Party's services for any and only business need. As these Third Parties might access physically or technically any kind of information that SAMOS STEAMSHIP is liable for, contractual agreements established include minimum security measures appropriate to the services provided, as well as appropriate contractual clauses dictated by Article 28 of GDPR.

This section of the policy mentions some of the safeguards that are taken into consideration to be included in the contractual agreements:

- Service description;
- Security measures;
- Non-disclosure agreements;
- Roles and responsibilities;
- Target service levels;
- Contacts and reporting lines;
- The right for second party audits.

16. Protection of Individual Rights

16.1 Data Subject Requests Procedure

Data subjects have access rights to their personal information irrespective of when the record was created

To exercise this right, an individual makes a request for information, by email (gdpr@samossteamship.gr) addressed to the DP Coordinator, which logs each request as it is received.

SAMOS STEAMSHIP respects and facilitates the exercise of data subject rights related to:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

Subject access requests can be made by:

- The individuals themselves
- A duly authorized representative appointed by the individual to act on their behalf such as solicitors or a relative. In certain situations, the court granted an attorney on behalf of an adult who is incapable of consent [judicial protection of incapable adults].

This procedure applies to all requests for access to personal data held by SAMOS STEAMSHIP.

The DP Coordinator aims to:

- provide the relevant data within 30 days of the receipt of the written request from the Data Subject.
- always verifies the identity of anyone making a subject request, whether this is the individual, legal guardian or law enforcement agent (with appropriate jurisdiction), before handling over any information.
- records details of the identification check, along with the request, in the “Data Subject Request Log” which is kept by Data Protection Coordinator.

Any staff member who receives such a request for information, immediately forwards it to the DP Team/DP Coordinator without any other action and deletes any copy. Otherwise, he/she will be fully responsible for any breach of silence.

16.2 Request for Data Rectification (GDPR Art. 16)

Data Subjects have the right to request SAMOS STEAMSHIP to correct or supplement erroneous, misleading, outdated, or incomplete personal data.

Once identification of the data subject has been confirmed, data on the individual is to be updated and SAMOS STEAMSHIP confirms by email, accordingly.

The request is recorded in the Data Subject's Request Log.

16.3 Request for Erasure (GDPR Art. 17)

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request.

The request is recorded in the Data Subject Request Log.

An erasure request can only be refused if an exemption applies.

SAMOS STEAMSHIP is obligated to erase personal data where one of the following applies:

- personal data is no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- the data subject withdraws consent and no other legal basis for processing exists;
- the data subject objects to the processing carried out on the grounds of the data controller's legitimate interests and there are no other overriding legitimate grounds for the processing;
- the personal data has been unlawfully processed.
- personal data is not updated

If the request to erase personal data has been received and:

- identity has been confirmed,
- the request meets one of the above requirements and
- there is no legal contrary reason for processing,

SAMOS STEAMSHIP deletes the relevant data in its entirety and informs data subject accordingly.

Key steps in erasing data:

- the DP Team/DP Coordinator is responsible for overseeing execution of the request;

- the request and evidence are recorded in the request log;
- data owner and DP Team/DP Coordinator are responsible for locating all relevant personal data with due diligence searches on all databases, mailing lists and general file stores etc and deleting them from all locations;
- An email is sent to the data subject confirming that data has been removed and processing has therefore ceased, unless it proves impossible or involves disproportionate effort.

16.4 Right to Object to Processing (GDPR Art. 21)

The data subject has the right to object at any time to processing of personal data unless:

- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party.

In determining whether or not to approve an objection, SAMOS STEAMSHIP must consider:

- to demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject (for safety & security reasons included) or
- for the establishment, exercise or defense of legal claims.

When such grounds do not exist, the processing must cease immediately.
Data subjects have the right not to be subject to a decision based solely on automated processing.

16.5 Request for Data Portability (GDPR Art.20)

Upon request a data subject has the right to receive a copy of their data in a structured format.

These requests are processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals.

A data subject may also request that their data is transferred directly to another system if only this is technologically feasible. In this case, the transfer of the data is done for free.

If SAMOS STEAMSHIP cannot respond fully to the request within 30 days, the DP Team/DP Coordinator nevertheless provides the following information to the data subject or their authorized legal representative within the specified time:

- An acknowledgement of receipt of the request.
- Any information located to date.
- Details of any requested information or modifications which are not provided to the data subject, the reason(s) for the refusal, and any procedures available for appealing the decision.
- An estimated date by which any remaining responses are provided.
- An estimate of any costs to be paid by the data subject (e.g. where the request is excessive in nature).
- The name and contact information of the contact person.

17. Transfer of Personal Data (GDPR Art. 45-49)

Data transfers within the EU

During data transfer of personal data within the EU, Samos Steamship assesses whether the transfer of personal data from one company to another is lawful under the Art. 6 of the GDPR.

Data transfers outside the EU to third parties

Cross-Border Data Transfers to a recipient in a third country take place if the third country receives an Adequacy Decision from the Commission.

Regarding transfers to the US, the EU-US Privacy Shield provides an adequate level of data protection.

If no adequacy decision is available, the adequate level of data protection is ensured by Samos Steamship through:

- Standard contractual clauses (Article 46 (2) c) and d) GDPR): Samos Steamship uses standard contractual clauses for transfers of personal data outside the EU. The standard contractual clauses set the obligations of both the exporter and the importer of data. Both parties make provision in the contract for those technical and organisational measures which, having regard to applicable data protection law, the state of the art and the cost of their implementation, are necessary in order to protect personal data against accidental or unlawful destruction or

accidental loss, alteration, unauthorised disclosure or access or any other unlawful forms of processing.

- Individually negotiated contractual clauses (Article 46 (3) GDPR): Samos Steamship may also use individually negotiated agreements for the transfer of data to a third country. These agreements are approved by the responsible supervisory authority (Article 63 GDPR).

In the absence of an adequacy decision pursuant to Article 45(3), or of the above appropriate safeguards under Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation takes place on one of the following conditions:

1. the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

2. the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data Rec.111 Art.49(1)(b), subject's request;

3. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

4. the transfer is necessary for important reasons of public interest;

5. the transfer is necessary for the establishment, exercise or defence of legal claims;

6. the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

7. the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

18. Responsibilities

Each individual or team that handles personal data ensures that it is handled and processed in line with this policy, data protection principles and any relevant company's policies (i.e. cyber security).

However, the relation between responsibility and key managerial position is as follows:

Managerial Position	Responsibilities
Management	SAMOS TEAMSHIP's management is ultimately responsible for ensuring that the company meets its legal obligations.
Data Protection Team/ Coordinator	The Data Protection Team(DPT)/Coordinator, is responsible for: Keeping the SAMOS TEAMSHIP's management updated about data protection responsibilities, risks and issues. Reviewing all data protection training and advice for SAMOS TEAMSHIP's employees. Handling data protection questions from data subjects (employees, third parties etc.). Dealing with requests from individuals to see the data the company holds about them (also called "data subjects' requests"). Checking and approving any contracts or agreements with third parties that may handle special categories of personal data. Cooperate with the Hellenic DPA and report any data breach

IT Manager	The IT Manager is responsible for: Ensuring all systems, services and equipment used for storing data meet acceptable security standards. Performing regular checks and scans to ensure security hardware and software in functioning properly. Evaluating any third-party services, the company is considering using to store or process data. For instance, cloud computing services.

19. Reporting Breaches

All members of staff have an obligation to report actual or potential data protection compliance failures due and must immediately notify the DP Team/DP Coordinator providing a description of what has occurred.

Notification of the incident can be made via e-mail gdpr@samossteamship.gr or by calling +30 210 9465900.

This allows us to:

- Investigate the failure and take remedial steps if necessary
- Carry out a risk assessment to determine whether the risk to the rights and freedoms of data subjects to be affected is sufficiently high.
- Maintain a register of compliance failures
- Notify:

1. the Personal **Data Protection Authority (Hellenic DPA)** of any compliance failures that are material either in their own right or as part of a pattern of failures **within 72 hours**

2. The data subjects affected without undue delay, when the personal data breach results in high risk to the rights and freedoms of natural individuals.

The communication to the data subject is not required if any of the following conditions are met:

- the controller (SAMOS STEAMSHIP) has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal

data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption;

- the controller (SAMOS STEAMSHIP) has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1, is no longer likely to materialize;
- it involves disproportionate effort. In such a case, a public announcement or similar measure will take place whereby the data subjects are informed in an equally effective manner.

A personal data breach is notified to the supervisory Authority "unless the personal breach is unlikely to result in a risk to the rights and freedoms of natural persons" (GDPR Article 33).

The supervisory Authority for the purposes of the GDPR for «SAMOS STEAMSHIP» is as follows:

Name:	Hellenic Data Protection Authority (HDPA)
Address:	Kifissias 1-3, 115 23 Athens, Greece
Telephone:	+30-210 6475600
Fax:	+30-210 6475628
Email:	contact@dpa.gr

The notification to the supervisory authority shall:

- describes the nature of the personal data breach;
- the categories and approximate number of data subjects concerned;
- communicates the name and contact details of the DP Team/DP Coordinator or other contact point where more information can be obtained;
- describes the likely consequences of the personal data breach;
- describes the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
- describes the reasons why it was not given on time if the notification falls outside of the 72-hour timeframe.

Written confirmation should be obtained from the supervisory authority that the personal data beach notification has been received, including the date and time at which it was received.

SAMOS STEAMSHIP documents:

- any personal data breaches, including the facts relating to the personal data breach, its effects
- and the remedial action taken

The DP Team/DP Coordinator investigates all reported incidents to confirm whether or not a personal data breach has occurred.

Types of personal data breaches

- "Confidentiality breach" - where there is an unauthorized or accidental disclosure of, or access to, personal data.
- "Integrity breach" - where there is an unauthorized or accidental alteration of personal data.
- "Availability breach" - where there is an accidental or unauthorized loss of access to, or destruction of, personal data.

SAMOS STEAMSHIP shall assess the level of risk before deciding whether or not to notify.

The DP Coordinator with the assistance with the IT Manager determines the severity and the impact of the data breach. The severity of a personal data breach is defined, in the context of this Procedure, as the ***"estimation of the magnitude of potential impact on the individuals derived from the data breach"***.

Criteria

The main criteria taken into account while assessing the severity of a personal data breach are:

- **Data Processing Context (DPC):** Addresses the type of the breached data, together with a number of factors linked to the overall context of processing.
- **Ease of Identification (EI):** Determines how easily the identity of the individuals can be deduced from the data involved in the breach.
- **Circumstances of breach (CB):** Addresses the specific circumstances of the breach, which are related to the type of the breach, including mainly the loss of security of the breached data, as well as any involved malicious intent.

Factors to be considered as part of this risk assessment should include:

- Whether the personal data was encrypted.
- The data items included (e.g. name, address, bank details, biometrics)
- The volume of data involved
- The number of data subjects affected
- The nature of the breach

Organizational units or roles involved in risk assessment include representatives from the following areas depending on the nature of the personal data breach:

- Senior Management
- IT Manager
- Data Protection Team
- Business departments which are affected by the breach

20. Collection of Evidence Procedure

SAMOS STEAMSHIP in order to show compliance with the EU General Data Protection Regulation (GDPR), produces and maintains a wide range of documentation.

SAMOS STEAMSHIP retains, at the minimum, the following critical documents:

- Templates for creating clear and accurate privacy notices
- Data breach notification forms and procedure
- Data subject request templates and procedures
- An international data transfer procedure
- Consent form templates
- Data protection impact assessment templates
- Important information security policies and procedures to keep information secure.

21. Data Processing Agreement

A data processing agreement is needed when:

- SAMOS STEAMSHIP uses a data processor (a third party who processes personal data on behalf of the controller/Samos Steamship).
- A data processor employs another processor (sub-processing).

By having a contract in place with the required terms, SAMOS STEAMSHIP ensures the compliance with the GDPR i.e. the protection of the personal data of charterers, staff and other parties since the agreement sets out what the processor is expected to do with the data.

The agreement (or other legal act) includes – at least- the following details about the processing:

- the subject matter;
- how long it is to be carried out for;
- what processing is being done;
- its purpose;
- the type of personal data;
- the categories of data subjects; and
- the obligations and rights of the data controller.

22. Prohibited Activities

The following activities are strictly prohibited:

- using data obtained for one purpose for another supplemental purpose (for example, using contact details provided for HR-related purposes for marketing purposes)
- disclosing personal data to a third person outside of the company without the consent of the data subject.

23. CCTV Maintenance

SAMOS STEAMSHIP aims at the following regarding CCTV:

- ensuring that those capturing individuals' information comply with the GDPR and other relevant statutory obligations;
- contributing to the efficient deployment and operation of the camera system;
- meaning that the information captured is usable and can meet its objectives in practice;
- reducing reputational risks by staying within the law and avoiding regulatory action and penalties;
- re-assuring those whose information is being captured.

SAMOS STEAMSHIP owns and operates a CCTV network for the purposes of crime prevention, detection, and safeguarding of assets. Where a data subject is identified, images are processed as personal data.

CCTV recordings and other logs are stored securely and encrypted wherever possible. Recorded material is stored in a way that maintains the integrity of the information.

Individuals have the right to request a copy of any CCTV footage in which they are in focus and/or clearly identifiable. If the request is valid and permissible, the company supplies the individual with that footage within 30 days of the validation. The same is true of other kinds of data relating to employee monitoring.

SAMOS STEAMSHIP discloses to employees that CCTV is in use and that they are captured on footage obtained. SAMOS STEAMSHIP placed signs at the entrance to the surveillance system's zone and reinforcing this with further signs inside the area.

Disclosure of information from surveillance systems is controlled and consistent with the purpose(s) for which the system was established. Recorded images are viewed in a restricted area. The monitoring or viewing of images from areas where an individual has an expectation of privacy is restricted. Offices are not monitored.

SAMOS STEAMSHIP does not keep information for longer than strictly necessary to meet its purposes for recording it.

Data privacy impact assessment (DPIA) is performed when needed. DPIAs looks at the pressing need that the surveillance system is intended to address and whether its proposed use has a lawful basis and is justified, necessary and proportionate.

24. Fingerprints

Personnel of SAMOS STEAMSHIP can choose the way of entry into its head offices. One of the choices is via fingerprint. The relevant policy is kept internally.

25. GDPR Training –Objectives:

- Ensure all relevant staff have adequate and up to date training on data protection regulations and GDPR changes
- All staff receives mandatorily training on this policy.
- New joiners receive training as part of the induction process.
- Further training is provided whenever there is a substantial amendment in the law or our policy and procedure.

26. Monitoring of the Effectiveness of the Policy

Everyone must observe this policy.

The management team of SAMOS STEAMSHIP ensures that all SAMOS STEAMSHIP employees responsible for the processing of Personal Data are aware of and comply with the contents of this Privacy Policy and all relevant policies and legislation.

The DP Team/DP Coordinator has overall responsibility for this policy, regularly monitors it to make sure it is being adhered to. Any amendments are communicated to SAMOS STEAMSHIP's employees by the DP Team/DP Coordinator.

The DP Team/DP Coordinator carries out an annual data protection compliance audit for SAMOS STEAMSHIP to confirm adequate level of compliance including:

- The conformity of employees' activities.
- The assignment of responsibilities.
- Raising awareness.
- Training of employees.

The DP Coordinator, in cooperation with key company personnel, arranges a plan with a schedule for correcting any identified deficiencies within a defined and reasonable time frame.

Any major deficiencies identified are reported to and monitored by SAMOS STEAMSHIP Management team.

SAMOS STEAMSHIP makes sure all third parties engaged to process Personal Data on SAMOS STEAMSHIP's behalf are aware of and comply with the contents of this Privacy Policy and all relevant policies and legislation.

Assurance of such compliance is obtained from all third parties, whether companies or individuals, prior to granting them access to Personal Data controlled by SAMOS STEAMSHIP.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action by the DPA.

This Privacy Policy is available to all SAMOS STEAMSHIP's employees as deemed appropriate by the DP Coordinator.

All inquiries about this Privacy Policy, including requests for exceptions or changes are directed to the DP Team/DP Coordinator via e-mail gdpr@samossteamship.gr.