GLOBAL POLICY ON PERSONAL INFORMATION PRIVACY

CONTENT:

IMPORTANT NOTICE: *This global policy applies to set the basic standards regarding the processing of personal data by you in the course of your work for Seapeak. Please be mindful that these basic standards will apply globally to the extent not in conflict with local law restrictions. The Policy is subject to the more onerous data protection obligations that local laws may impose upon Seapeak and its Group companies. In that regard, for details of particularities relating to the EU General Data Protection Regulation (GDPR) or the UK General Data Protection Regulation (UK GDPR) please see below Section 15.*

---

1. INTRODUCTION

1.1. Background

This Personal Information Privacy Policy ("**Polic**y") set out how Seapeak L.L.C. and its subsidiaries (collectively "**Seapeak**", "**we**", "**our**" or "**us**") handle the personal information of individuals.

We are committed to meeting high standards when servicing the needs of our employees, customers and other third parties. As these activities often involve the collection, use and disclosure of personal information about our employees, customers and other relevant data subjects, protecting their personal information is very important to Seapeak.

1.2. Definitions

"**Personal information**" is any information identifying a data subject or information relating to a data subject that we can identify (directly or indirectly) from that information alone or in combination with other identifiers we possess or can reasonably access. Personal information includes special categories of personal information and pseudonymised personal information but excludes anonymous information or information that has had the identity of an individual permanently removed. Personal information can be factual (for example, a name, address, email address, telephone number, location, date of birth, payment card data, identification number such as social security or tax ID number, driver's license number, medical and health-related information) or an opinion about that person's actions or behaviour.

> *"Explanatory Note: It is important to understand that personal information concerns information about individuals – not companies or other legal entities – although information about individuals within those companies and legal entities will be their personal information. It is also important to understand that*

personal information is not restricted to information about the personal/home lives of individuals. Information about individuals acting in a work or official capacity may also be personal information."

"**Processing**" is very widely defined to include all operations relating to personal information. This includes all activity from the point of collection to the point of destruction/erasure. Even the mere holding or storage of personal information is processing and, therefore, a regulated activity under the relevant data protection law.

1.3. Purpose

The purpose of this Policy is to outline the principles and practices we will follow worldwide to collect, use and protect the personal information of our employees, customers and other data subjects. This Policy applies to personal information held by Seapeak and its direct and indirect subsidiaries ("**Group Companies**") and their employees and to personal information held or processed on their behalf by third parties. This Policy sets out what we expect from our employees, contractors and other relevant third parties in order for Seapeak and Group Companies to comply with the applicable data protection law. Compliance with this Policy is mandatory for all our employees and any contractors who work for us. Any breach of this Policy may result in disciplinary action or (in the case of contractors) be viewed as a material breach of contract. The Policy is subject to the more onerous data protection obligations that local laws may impose upon Seapeak and Group Companies.

1.4. Commitment

Our privacy commitment is to process personal information of employees, customers and other relevant data subjects only for lawful purposes in accordance with the following privacy principles to ensure the accuracy, lawfulness, fairness, transparency, confidentiality and security of such personal information and to allow our employees, customers and other data subjects to exercise their right in accordance with the relevant data protection law (as, for example, the request for access to, and correction of, their personal information).

1.5. Related policies

Related policies, procedures and guidelines are available to help you interpret and act in accordance with this Policy and are listed in Appendix I. You must also comply with

all such related policies, procedures and guidelines.

2. IMPORTANCE OF COMPLIANCE

The correct and lawful treatment of personal information will maintain confidence in Seapeak and its Group Companies, will provide for successful business operations, and will maintain our reputation. As importantly, it also protects the individual, whose personal information we process, from harm. Protecting the confidentiality and integrity of personal information is a critical responsibility that we take seriously at all times. If we fail to comply with data protection laws, then we may be subject to substantial sanctions and reputational damage.

3. ACCOUNTABILITY

3.1. Privacy Officer

The Privacy Officer and the Privacy Liaison Group (see Section 13 below and Appendix II attached) are responsible for ensuring our compliance with this Policy. The Privacy Officer may delegate various responsibilities in this regard to the members of the Privacy Liaison Group and other individuals within our organisation.

3.2. Responsibility of all

All individual business units and departments are responsible for ensuring all employees and contractors comply with this Policy and they must implement appropriate practices, processes, controls and training to ensure such compliance. If you have management responsibility, you are expected to regularly review all the systems, processes and procedures under your control to ensure they comply with this Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of personal information.

3.3. Transfer to third party

Where personal information is transferred to any party outside Seapeak or Group Companies, there should always be an agreement in place between the company transferring the information and the third party receiving the information to ensure compliance with information protection obligations. In such instances our Legal

Department should be contacted for assistance in preparing appropriate forms of agreement.

4. IDENTIFYING PERSONAL INFORMATION

As noted, personal information is, with only limited exception, any information about an identifiable person. Examples of employee personal information include information in contracts of employment; bank account details and details of next-of-kin. When in doubt as to whether or not any information amounts to personal information, guidance should be sought from the Privacy Officer.

5. DATA PROTECTION PRINCIPLES

5.1. Principles

The data protection principles (which, for ease of reference, are listed in Appendix III) require us to process personal information lawfully, fairly and in a transparent manner. We must only collect, process and share personal information for specified purposes. We will inform our employees, customers and third parties why and how we collect, use and disclose their personal information and obtain their consent where required.

5.2. Privacy Notices

To ensure compliance with these requirements, privacy notices have been prepared to explain how we process personal information we collect. These 2 privacy notices are accessible on our website. The first privacy notice explains the purposes for which we process personal information that we collect from data subjects who are external to our organisation. The second privacy notice explains the purposes for which we process the personal information of our employees. It is essential that we process all personal information in accordance with the terms of the relevant privacy notice and we are responsible for ensuring that you are aware of the terms of each privacy notice in so far as it is relevant to the performance of the personnel duties.

Often under applicable data protection law, there will be various legal justification that allow us to process personal information without consent but, where necessary, we will obtain the employee, customer and other data subject consent to collect, use or disclose personal information.

6. DATA MINIMISATION

We will collect personal information by fair and lawful means and limit the amount and type of information collected for the purposes identified. Thus, we must ensure that personal information must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

All forms through which personal information is gathered (such as employment application forms, website feedback forms etc.) should contain suitable wording covering all intended uses of the information and refer to/link with the relevant privacy policy (see Section 5 above). Copies of such forms should be retained in all cases in accordance with our Records Management Policy.

Personal information obtained should only be that necessary in order to fulfill the specified purposes and should be retained if necessary for efficient operation of our business, human resources administration or if required by local law.

We may only process personal information when performing our job duties requires it. We cannot process personal information for any reason unrelated to our job duties. The personal information protection requirement principles require that we do not collect excessive personal information. We need to ensure that any personal information we collect is actually required for the intended purpose for which we will process it. In addition, you should obtain your supervisor's approval before joining an industry organisation as a representative of Seapeak.

7. LIMITING USE, DISCLOSURE, RETENTION AND CONTROLLING TRANSFER

We will not use or disclose employee, customer or other data subject personal information for purposes other than those for which it was collected except with the consent of the individual or as required by law.

We must not keep personal information in a form which permits the identification of the corresponding data subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements (For more details, please see our Records Management Policy). Subject to any applicable business legal or regulatory requirements, we will not keep personal information longer than necessary to fulfil the specified identified purposes and will ensure that such information is

deleted or destroyed in a secure manner. In this respect, Seapeak maintains retention policies and procedures (see the Records Management Policy) to ensure personal information is deleted after a reasonable time following the end of the purposes for which it was being held, unless law requires such data to be kept for a minimum time.

Regarding the transfer of employee, customer and other data subject personal information between Seapeak and amongst Group Companies, these transfers are subject to the relevant local data protection law (in particular, these transfers may be subjected to the GDPR requirements – for more details please Section 15) and, in any case, the following considerations will apply:

- the processing of personal information will be carried out in accordance with this Policy and/or local laws (if the latter are more onerous than the terms of this Policy) that apply to the employees or Group Companies transferring the data. Clear instructions will be given by the information transferor's employees to process personal information only in accordance with the requirements of local laws;
- personal information will only be transferred if necessary for efficient human resource administration or operation of Seapeak or Group Companies, every effort will be made to ensure the security of any personal information being transferred;
- employees or Group Companies receiving or requesting information will notify the employee transferring the personal information about any legally binding request for disclosures of the personal information (e.g., by a law enforcement authority); and
- all data processing facilities, systems and operations of Seapeak and Group Companies will be subject to being audited for compliance with this Policy.

8. ACCURACY

Personal information must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate. Therefore, you must ensure that employee, customer or other data subject personal information is accurate, current and complete where it may be used to make a decision impacting the employee, customer or other data subject or, if permitted by law and this Policy, disclosed to another organization.

9. STORAGE AND SAFEGUARDS

Personal information may be held in electronic records and in manual records (*e.g.*, paper files microfilm and other media). Some examples of where personal information may be found include:

- employment files;
- databases containing contact details of individuals (*e.g.*, contact details of individuals who work for customers); and
- mailing lists.

We must ensure that all personal information that we process as part of our work duties are stored in our systems (or, for paper records, in our premises). No personal information should be held anywhere else.

We will use appropriate technological, physical and organizational measures appropriate to the sensitivity of the information to safeguard individuals' personal information in any format against accidental loss, destruction, theft, unauthorized access, unlawful processing or damage. Third parties of which we are aware who obtain possession of employee, customer and other data subject personal information will be required to respect the relevant data protection law and the confidentiality of such information and all requirements of local laws.

Personal information held on computers will be protected by strict security measures, and manual records containing the personal information of any individual will be kept locked with access strictly controlled in our premises.

When it is being discarded, material containing personal information should be shredded or otherwise disposed of in a secure manner.

We have put in place procedures to deal with any suspected personal information breach and will make appropriate notifications where we are legally required to do so (see our Data Incident Management Procedures).

---

10. OPENNESS

We will make available to employees and customers information about our policies and practices relating to the management of employee, customer and other data subject personal information upon written request.

---

11. INDIVIDUAL ACCESS

11.1. Subject to exceptions under applicable law, upon request we will provide employees, customers or other data subjects with copies of their personal information and tell them to whom their personal information has been disclosed, if applicable, and how it was used in such disclosure. Paragraphs 11.2 and 11.3 apply to requests by employees.

11.2. Subject to paragraph 11.3, and after first discussing an access request with an appropriate member of the Privacy Liaison Group and submitting a written access request to such member of the Privacy Liaison Group, employees will be informed of the existence, use and disclosure of their personal information, and be given reasonable access to that information.

11.3. Notwithstanding paragraph 11.2 and to the extent not in conflict with local privacy law restrictions, if we deem it appropriate (*e.g.*, in situations involving solicitor-client privilege or disclosures that would reveal personal information about another individual or involve health and safety concerns) or other situations permitted by law, we may, in writing to the requesting employee, deny access requests in whole or in part advising of the reason(s) for the denial and the recourse available to the requesting individual. All legitimate written requests to obtain access or exercise other rights in relation to personal information in our possession and which have first been discussed with an appropriate member of the Privacy Liaison Group will be dealt with within the relevant time stipulated by data protection law.

11.4. If you receive a request from an external individual such as a customer, you must immediately notify a member of the Privacy Liaison Group so it can be dealt with appropriately.

11.5. When permitted by law, a minimal fee may be charged for providing access to personal information. Where a fee may apply, we will inform the requesting individual of the cost and request further direction from the requesting individual as to whether or not we should proceed with the request. We will make available to employees and customers information about our policies and practices relating to the management of employee, customer, and other data subject personal information upon written request.

12. DATA PROTECTION IMPACT ASSESSMENT (DPIA)

When we are considering projects to implement major system or business change programs involving the processing of personal information or any other activity which will involve (or may potentially involve) the processing of personal information which has not been collected before or the processing of personal information in new ways or for new purposes; then the Privacy Officer must be advised accordingly at an early opportunity in order that he/she can consider the proposed project or activity and determine whether a data protection impact assessment is required.

---

13. RESOLVING YOUR CONCERNS AND CONTACTING THE PRIVACY OFFICER

By the appointment of a Privacy Officer and the establishment of the Privacy Liaison Group, we will maintain procedures for addressing and responding to inquiries or complaints about our handling of employee, customer and other data subject personal information.

Employees and other relevant data subjects should direct any complaints, concerns or questions regarding our compliance with this Policy in writing to the Privacy Officer as follows:

Michel Nielsen
Privacy Officer
Email: Michel.Nielsen@seapeak.com

When an employee, customer or data subject demonstrates the inaccuracy or incompleteness of personal information in our possession, we will correct or update such information as required. As with requests for access, requests for rectification of personal information must first be addressed verbally and then in writing with an appropriate member of the Privacy Liaison Group. If you receive a request from an external individual such as a customer you must immediately notify a member of the Privacy Liaison Group so it can be dealt with appropriately.

The Privacy Officer or an appropriate member of the Privacy Liaison Group must be immediately contacted in the following circumstances:

- if an employee is unsure whether particular processing will be within the terms of the relevant privacy notice or are otherwise unsure of the lawful basis which you are relying on to process personal information;

- if an employee is unsure about the retention period for the personal information being processed;
- if an employee is unsure about what security or other measures you need to implement to protect personal information;
- if there has been a personal information incident (for more details and for any personal information incident please follow the procedures of our Data Incident Management Procedures);
- if an employee is unsure whether we are permitted to transfer personal information;
- if an employee receives any communication from an individual which may seek to exercise any rights which he/she may have under the relevant data protection law;
- whenever an employee is engaging in a significant new, or change in, processing activity or plan to use personal information for purposes others than for which it was collected;
- if an employee is considering entering into any contracts with third parties (including our vendors) which shall involve the disclosure or sharing of personal information; or
- if an employee plans to undertake any activities involving automated processing including profiling or automated decision-making.When we are considering projects to implement major system or business change programs involving the processing of personal information or any other activity which will involve (or may potentially involve) the processing of personal information which has not been collected before or the processing of personal information in new ways or for new purposes; then the Privacy Officer must be advised accordingly at an early opportunity in order that he/she can consider the proposed project or activity and determine whether a data protection impact assessment is required.

14. EXCEPTIONS, QUALIFICATIONS, AMENDMENTS

Although not set out in this Policy, we will rely on any exemptions or qualifications that are either contained in applicable legislation or used by us in good faith as permitted by law. We may amend this Policy from time to time, as we deem necessary. Where changes are made, we will notify you, but it is your responsibility to check back regularly to obtain the latest copy of this Policy.

This Policy does not override any applicable national data privacy laws and regulations in countries where we operate.

15. SPECIFIC REFERENCE TO THE EU GDPR

15.1. Scope.

The European Union (EU) General Data Protection Regulation 2016/679 ("GDPR") is a European Union data protection law which came into effect on 25 May 2018. The GDPR is retained in the United Kingdom ("UK") domestic law as the UK General Data Protection Regulation ("UK GDPR"). The GDPR applies to the processing of personal information:

- in the context of activities of establishments within the European Economic Area ("EEA", *i.e.*, the member states of the EU together with Iceland, Liechtenstein and Norway) and the UK;
- of individuals within the EEA/UK by non-EEA establishments where the processing activity relates to the offering of goods and services to those individuals or to the monitoring of their behaviour within the EEA/UK; and
- on vessels which are flagged under a flag of a state of the EEA/UK.

Clearly, the GDPR does not apply to all processing of personal information carried out by Seapeak and Group Companies.

In circumstances where the GDPR does apply to particular data processing in accordance with these rules, the individuals whose personal information is being processed have the following rights under the GDPR:

- **Access to personal information:** Individuals have the right to request a copy of the personal information about them that we hold.
- **Correcting personal information:** Individuals may ask us to correct any personal information about them that is inaccurate, incomplete or out of date.
- **Deletion of personal information:** Individuals have the right to ask us to delete personal information about them where:
  - They consider that we no longer require the information for the purposes for which it was obtained.
  - We are using that information with their consent and that consent has been withdrawn (see below - Withdrawing consent to using personal information).
  - They have validly objected to our use of their personal information (see below - Objecting to how personal information is used)
  - Our use of the individual personal information is contrary to law or our other legal obligations.

- **Objecting to how personal information is used:** Individuals have the right at any time to require us to stop using their personal information for direct marketing purposes. In addition, where we use personal information of an individual to perform tasks carried out in the public interest or on the basis of legitimate interests then, if the individual asks us to, we will stop using that personal information unless there are overriding legitimate grounds to continue.
- **Restricting how we may use personal information:** In some cases, individuals may ask us to restrict how we use their personal information. This right might apply, for example, where we are checking the accuracy of personal information that we hold or assessing the validity of any objection made by an individual to our use of their information. The right might also apply where there is no longer a basis for using an individual's personal information, but they don't want us to delete the data. Where this right is validly exercised, we may only use the relevant personal information with the individual's consent, for legal claims or where there are other public interest grounds to do so.
- **Portability:** If we process personal information that has been provided to us on the basis of consent or because it is necessary for the performance of a contract to which the individual is a party, and in either case that processing is carried out by automated means, then the individual has the right to have that personal information sent to them in a machine-readable format. Where technically feasible, the individual also has the right to have that personal information transmitted directly to another controller.
- **Automated processing:** If we use personal information on an automated basis to make decisions which significantly affect an individual, that individual has the right to ask that the decision be reviewed by an individual within our organisation to whom representations may be made concerning the decision or to contest it. This right only applies where we use information with the individual's consent or as part of a contractual relationship with the individual.
- **Withdrawing consent to using personal information:** Where we use personal information with individual consent the individual may withdraw that consent at any time and we will stop using that personal information for the purpose(s) for which consent was given.

For queries as to whether the (UK) GDPR applies to the processing of personal information or, if the (UK) GDPR does apply, and you wish to exercise any of these rights then please contact the Privacy Officer or an appropriate member of the Privacy Liaison Group.

15.2. Consent.

Please remember that, pursuant to the GDPR, for consent to be valid it must be freely given, specific, informed and be an unambiguous indication of the employee's wishes by which they, by a statement or by a clear positive action, signifies agreement to the processing of personal information relating to them.

15.3. Transfers.

Please also bear in mind that the GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of personal information protection afforded to individuals by the relevant EU data protection law is not undermined. We transfer personal information originating in one country across borders when we transmit, send, view or access that data in or to a different country.

15.4. Employee Information.

Seapeak group being a global organisation, personal information of employees which is subject to the GDPR may be accessible outside the EEA subject to suitable safeguards. In this respect, personal information may be accessed for any of the purposes set out in our employee privacy statement by a restricted number of individuals of our staff, agents or contractors from a country outside the EEA, in which data protection laws may be of a lower standard than in the EEA. We will ensure that any of your information that is accessible outside the EEA is handled subject to appropriate safeguards and in accordance with the GDPR.

Under the (UK) GDPR, we may only transfer personal information outside the EEA if one of the following conditions applies:

- the European Commission or the UK has issued a decision confirming that the country to which we transfer the personal information ensures an adequate level of protection for the data subjects' rights and freedoms;

Explanatory Note: *Countries for which the European Commission has issued adequacy decisions can be found at https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en. The European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man,*

Japan, Jersey, New Zealand, Switzerland, United Kingdom and Uruguay as providing adequate protection.

- appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission (sometimes called 'model form clauses'), an approved code of conduct or a certification mechanism, a copy of which can be obtained from the Legal Department or Privacy Officer;
- the data subject has provided explicit consent to the proposed transfer after being informed of any potential risks; or
- the transfer is necessary for one of the other reasons set out in EU data protection law including the performance of a contract between us and the data subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving consent and, in some limited cases, for our legitimate interest.

15.5. Sharing personal information.

Generally, we are not allowed to share personal information with third parties unless certain safeguards and contractual arrangements have been put in place (in this respect, please contact our Legal Department or Privacy Officer). We may only share the personal information we hold with another employee, agent or representative of Seapeak and Group of Companies if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

We may only share the personal information we hold with third parties, such as our service providers if:

- They have a need to know the information for the purposes of providing the contracted services;
- sharing the personal information complies with the relevant privacy notice provided to the data subject;
- the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- the transfer complies with any applicable cross border transfer restrictions;
- a fully executed written contract that contains GDPR mandated third party clauses has been obtained;
- the Privacy Officer has authorised the data sharing.

Fines under the GDPR: Please mind that infringements of the GDPR are subject to administrative fines of up to EUR 20,000,000 or 4% of total worldwide annual turnover of the preceding financial year (whichever is higher) and will cause a reputational damage to Seapeak.

APPENDIX I - RELATED POLICIES, PROCEDURES AND GUIDELINES

- Processing Conditions Guide
- Records Management Policy
- Data Protection Impact Assessment Policy and Data Protection Impact Assessment Procedures
- Data Incident Management Procedures
- Information Security Questionnaire
- Procedures for Responding to Personal Information Requests
- Data Incident Management Procedures
- Personal Information Breach Reporting Policy

APPENDIX II – PRIVACY LIAISON GROUP

(Membership subject to change from time to time)

Area of Responsibility	Privacy Liaison	Title	Contact Details
SHORE STAFF			
UK	**Jennifer Small**	Director, Human Resources	Jennifer.Small@seapeak.com +44 141 222 9019 Seapeak Maritime (Glasgow) Limited
Spain	**Jose Villasante**	Director, Marine HR	Jose.Villasante@seapeak.com +34 917 102 925 Seapeak Maritime Spain, S.L.U.
SEAFARERS			
Seapeak	**Colin Barr**	Head of Marine HR	Colin.Barr@seapeak.com Seapeak Maritime (Glasgow) Limited
Spain	**Jose Villasante**	Director, Marine HR	Jose.Villasante@seapeak.com +34 917 102 925 Seapeak Maritime Spain, S.L.U.
PRIVACY OFFICER, LEGAL, IT & RAC			
Privacy Officer Legal Compliance	**Michel Nielsen**	Associate General Counsel Privacy Officer	Privacy.Officer@seapeak.com +352 26 4958 4275 Seapeak Luxembourg S.à r.l.
RAS	**Steven Dibble**	Manager, Internal Audit•	steven.dibble@seapeak.com +1 604 609 6427 SP Maritime (Canada) Inc.
IT	**Jurgen Figura**	Chief Information Officer	Chief Information Officer +1 604 609 2953 SP Maritime (Canada) Inc.

APPENDIX III - DATA PROTECTION PRINCIPLES

Personal information shall be:

a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('***lawfulness, fairness and transparency***');

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes (***'purpose limitation'***);

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (***'data minimisation***');

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal information that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('***accuracy***');

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal information are processed; personal information shall be stored in accordance with our Records Management Policy (***'storage limitation'***);

f) processed in a manner that ensures appropriate security of the personal information, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (***'integrity and confidentiality***').