External Privacy Policy

Version 1.0 DRAFT

Last updated: March 5, 2026

Table of Contents

1. Purpose & Scope

Seabras Group, LLC and its subsidiaries, including Seabras 1 USA, LLC ("**Seabras US**") and Seabras 1 Brasil Ltda. ("**Seabras Brasil**"), collectively, "**Seaborn**" "**we**," "**our**" or "**us**," have adopted this External Privacy Policy ("**External Privacy Policy**") to describe the types of Personal Data we collect, process, maintain, protect and share, including information about the rights and choices you may have when it comes to your Personal Data.

This External Privacy Policy applies to those who use or interact with Seaborn's services, networks, platforms, and our website. It also applies to Personal Data we collect from third parties, including customers, potential customers, vendors, potential employees, and former employees ("**Data Subject**," "**you**," or "**your**") as part of our normal business operations, including activities relating to marketing, selling, negotiating, contracting, providing, implementing, supporting and billing services, and your physical or logical access to Seaborn offices, facilities and/or equipment.

2. Privacy Around the World

Seaborn operates and delivers services in multiple jurisdictions. This External Privacy Policy is governed by the data privacy and protection ("DPP") legislation of the country applicable to you ("**applicable DPP Law**"). In the event of any conflict between this External Privacy Policy, a separate agreement between you and Seaborn, and applicable DPP Law, the order of priority is the applicable DPP Law, the terms of the separate agreement, and this policy.

In particular, this External Privacy Policy will draw your attention to distinct obligations to Brazil Data Subjects under the Brazil LGPD and California Data Subjects under the CCPA.

a) The Brazil LGPD specific provisions, especially those contained in ***Annex A***, are *only applicable* to Data Subjects located in Brazil. They *do not apply* to California Data Subjects or Other Data Subjects.

b) The CCPA-specific provisions, contained in ***Annex B***, are *only applicable* to California Data Subjects. They *do not apply* to Brazil Data Subjects or Other Data Subjects.

Data Subjects requesting information about this External Privacy Policy or Data Subject rights may contact Seaborn using the contact information in Section 11 of this External Privacy Policy.

We provide the following table as a helpful summary of the key elements of this External Privacy Policy. You can obtain more details in the sections that follow.

Capitalized terms used in this External Privacy Policy have the meaning set forth herein. ***(See Glossary)***

SUMMARY TABLE	
Collected Personal Data	Seaborn may collect personal data such as first name and last name, identification information such as social security number, driver's license number, state-issued ID, and other information related to a Data Subject, as defined by applicable DPP Law. **…more**
Purposes of Processing	Personal Data is only collected and Processed for legitimate business purposes or as necessary to comply with the law, including for example: • Customer Acquisition and Prospecting • Performance and Fulfillment of Contracts • Service Provider Management • Promotion and Advertising of Services Provided by Seaborn • Collection of Payments and Other Unfulfilled Obligations • Compliance Obligations and Audits • Credit Risk Check • Vendor Selection and Management • Legal and Administrative Compliance • Defense of Seaborn's Rights and Interests • Control and Management of Access to Physical Premises and Logical Systems • Response to a Data Subject's Request • Fraud Prevention • Corporate Transactions • Compliance with Legal Obligations **…more**
Controller	The specific Seaborn entity serving as the Controller in a given situation will be determined by the particular circumstances, and may be one of the following companies: 1. **Seabras 1 USA, LLC** 600 Cummings Center, Suite 268Z, Beverly, MA 01915, USA 2. **Seaborn Management, LLC** 600 Cummings Center, Suite 268Z, Beverly, MA 01915, USA 3. **Seabras 1 Brasil Ltda.** CNPJ nº 17.289.520/0001-69, Av. Paulista, nº 352, 7º Andar, Conj. 77, CEP 01.310-905, Bela Vista, São Paulo **Brazil DPO**: Maria Beatriz M. de Miranda Tello –BrasilDPO@seabornnetworks.com **Global DPO**: Lin Gentemann – USDPO@seabornnetworks.com **...more**

SUMMARY TABLE	
Legal Basis for Processing Personal Data	The legal grounds under which Seaborn is lawfully authorized to Process Personal Data under applicable DPP Law include: • Legitimate Interest of the Controller. • Execution of a Contract or Preliminary Procedures. • Regular exercise of rights in judicial, administrative, or arbitration procedures. • Protection of Credit. • Compliance with a legal or regulatory obligation. • Fraud prevention and the Data Subject's safety. **...more**
Data Subject Rights	Data Subject rights are established by applicable DPP Law, based on which DPP Law you are subject to, which rights may include, for example: • Confirmation that we collect, use and/or Process Personal Data. • Access to Personal Data. • Correction or updating of Personal Data. • Deletion of Personal Data. **...more**

3. Glossary

Capitalized terms used in this External Privacy Policy have the meaning set forth below unless otherwise defined under applicable DPP Law.

3.1 Anonymization: means a technique by which data loses the possibility of being associated, directly or indirectly, with an individual, making it impossible to identify the Data Subject.

3.2 Brazil ANPD: means Brazil's National Data Protection Authority, a federal public administration body responsible for activities related to the protection of personal data and privacy, including oversight of compliance with the Brazil LGPD across the national territory of Brazil.

3.3 Brazil Data Subject: means a natural person to whom the Brazil LGPD applies.

3.4 Brazil DPO: means the person designated to act as the primary point of contact and communication channel between the Controller, the Brazil Data Subject and the Brazil ANPD regarding Personal Data matters, including requests and notifications. For purposes of this External Privacy Policy, the Brazil DPO is the individual listed in Section 11 below.

3.5 Brazil LGPD: means the Brazilian General Data Protection Law, Federal Law No. 13,709, published on August 14, 2018, regulating the Processing of Personal Data of Brazil Data Subjects, with the purpose of protecting fundamental rights of freedom, privacy, and the free development of the personality of natural persons. The Brazil LGPD can be found in full at: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

3.6 California Data Subject: means a natural person who is a California resident to whom the CCPA applies.

3.7 CCPA: means the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020.

3.8 Consent: As generally understood, and as specifically defined under the Brazil LGPD, means the free, informed and unequivocal manifestation through which the Brazil Data Subject agrees to the Processing of their Personal Data for a specified purpose.

3.9 Controller: As generally understood, and as specifically defined under the Brazil LGPD, means the natural person or legal entity responsible for decisions regarding the Processing of Personal Data. For example, under this External Privacy Policy, Seabras Brasil or Seabras US may be the Controller. Controller includes "business" as defined under the CCPA.

3.10 Customer: means a prospect or customer who, in any manner, enters (or considers entering) into contracts with a Seaborn entity for the provision of Seaborn's services. If the prospect or customer is a legal entity, the term Customer refers to the Data Subject who represents that legal entity, unless the applicable DPP Law requires otherwise.

3.11 Data Protection Officer (DPO): means either the Brazil DPO or the Global DPO.

3.12 Data Subject: As generally understood, means the natural person to whom the Personal Data being Processed refers. Applicable DPP Law will determine whether you are a Data Subject in a particular jurisdiction.

3.13 Former Employee: means a former employee of any Seaborn company.

3.14 Legal Basis: means, with respect to Brazil Data Subjects only, the legal grounds under which Seabras Brasil, in its capacity as a Processing Agent, is lawfully authorized to Process Personal Data under the Brazil LGPD. With respect to all other Data Subjects, Legal Basis means the legal grounds under which Seaborn is lawfully authorized to Process Personal Data under the applicable DPP Law.

3.15 Other Data Subject: means any Data Subject other than a Brazil Data Subject or California Data Subject.

3.16 Personal Data: As generally understood, and as specifically defined under the Brazil LGPD, Personal Data means information related to an identified or identifiable natural person. Applicable DPP Law will determine whether information is Personal Data in a particular jurisdiction. Personal Data includes "personal information" as defined under the CCPA. You may also see it characterized in the following manner: (a) "personal information" or "PI", such as name, address, telephone number, email address, RG (Brazilian ID), CPF (Brazilian individual taxpayer registry); and (b) "personally identifiable information" or "PII", such as an individual's personal preferences, time-tracking records, job description, and access logs to internet applications (date and time of using a specific internet application).

Some DPP Law, including the Brazil LGPD, establish an important subset of Personal Data referred to as "**Sensitive Personal Data**" that requires your special attention. Under the Brazil LGPD Sensitive Personal Data means information related to racial or ethnic origin, religious belief, political opinion, union membership, or membership in a religious, philosophical, or political organization, as well as data concerning health, sexual life, genetic or biometric data when linked to a natural person. Sensitive Personal Data requires heightened protections due to its sensitive nature and potential for harm if improperly disclosed or used.

3.17 Potential Employee: means any individual who expresses interest in working or providing services to Seaborn as an employee by submitting professional resumes through appropriate channels, but who was not ultimately hired by Seaborn.

3.18 Processing or Process: As generally understood, and as specifically defined under the Brazil LGPD, means any operation performed with Personal Data, whether automated or not. This includes the collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, storage, archiving, deletion, evaluation, or control of information, modification, communication, transfer, dissemination, or extraction of Personal Data.

3.19 Processing Agents: As generally understood, and as specifically defined under the Brazil LGPD, means the agents responsible for the Processing of Personal Data, namely the Controller and the Processor.

3.20 Processor: As generally understood, and as specifically defined under the Brazil LGPD, means the natural person or legal entity that performs the Processing of Personal Data on behalf of the Controller, following its instructions. Processor includes "service provider" and "contractor" as defined under the CCPA.

3.21 System: means any of Seaborn's Data Assets and/or IT Assets, which includes, without limitation, software, websites, networking equipment, electronic devices, among others.

3.22 Global DPO: means, except with respect to Brazil Data Subjects, the person designated to act as the primary point of contact and communication channel between the Controller, the Data Subject and applicable regulatory authority regarding Personal Data matters, including requests and notifications. For purposes of this External Data Policy, the Global DPO is the individual listed in Section 11 below.

3.23 User: means a natural person using a Seaborn platform or our website.

3.24 Vendor: means a prospect or vendor who, in any manner, enters (or considers entering) into contracts with a Seaborn entity for the provision of their services. If the prospect or vendor is a legal entity, the term Vendor refers to the Data Subject who represents that legal entity, unless the applicable DPP Law requires otherwise.

3.25 Visitor: means an individual who, in any way, interacts with Seaborn's premises, facilities and/or physical assets, including personal and/or vehicular access.

4. How is Personal Data Collected?

4.1 Our Methods for Collecting Customer and Vendor Personal Data: We collect Customer and Vendor Personal Data through a variety of channels. This includes information obtained from our Systems, emails and instant messaging applications, public databases, events in which we participate, and through queries to public administration databases, regulatory bodies, credit bureaus, clearing services, and the positive registry, particularly for fraud prevention purposes. Personal Data is also collected when the Customer contacts us through our available sales channels or when they request and use our services. Personal Data is also collected when the Vendor is engaging with Seaborn for purposes of marketing, contracting and providing us their services.

4.2 Our Methods for Collecting Potential Employee and Former Employee Personal Data: We collect Potential Employee and Former Employee Personal Data through the completion of forms, responses to questionnaires, and the submission of documents containing Personal Data, such as professional resumes.

4.3 Our Methods for Collecting User Personal Data: We collect User Personal Data when individuals browse our website, use our platforms or when they request and use our services.

4.4 Our Methods for Collecting Visitor Personal Data: We collect Visitor Personal Data through the completion of forms, responses to questionnaires, and the submission of documents containing Personal Data prior to granting physical and/or logical access to Seaborn owned or leased premises, cable landing stations, points of presence (PoPs) and data center (collectively, "**Facilities**"), and physical assets, including network, equipment, personal and vehicular access.

4.5 Automatically Collected Personal Data via Our Website: We collect certain files and information stored on your devices when you visit our website. These files, known as "cookies," help facilitate your experience and optimize the use of our website according to your interests, preferences and needs. If preferred, cookies can be disabled through the browser used to access our website.

4.6 Personal Data Types and Collection Methods. We provide additional information on Data Types and Collection Methods in **Section 5**.

5. What Personal Data Do We Process?

5.1 We Process Personal Data which is necessary to achieve legitimate business interests of Seaborn, as described in Section 6. To do so, we may collect some or all of the information, which may be considered Personal Data in your jurisdiction, listed in the chart below.

PERSONAL DATA TYPES & COLLECTION METHODS			
DATA GROUP	**COLLECTION METHOD**	**DATA SUBJECT**	**PROCESSED PERSONAL DATA/SENSITIVE PERSONAL DATA**
CONTACT DATA	Personal Data is collected through public databases, events in which Seaborn participates, or contact initiated by the Vendor, by the Customer through available sales channels.	Customer Vendor	Name, E-mail, Employer (Name of the Company), Phone Number, Country of Origin, Title (Job Position), Government-issued ID (e.g., CNH).
CONTRACT DATA	Personal Data is provided by Clients or Vendors through communication tools, such as contract management platforms, email, and/or instant messaging applications.	Customer Vendor	Name, E-mail, Employer (Name of the Company), Address, Phone Number, Country of Origin, Title (Job Position), Tax ID (e.g., CPF), Government-issued ID (e.g., CNH and/or Passport), Signature, Marital Status, I.P. Address (digital signatures).
ADVERTISING DATA	Personal Data is collected during events for the purpose of promoting Seaborn's services.	Customer	Name and Picture.
CANDIDATE DATA	Personal Data is submitted via email and/or recruitment and candidate selection platforms.	Potential Employee	Name, E-mail, Telephone, Address, Age, Country of Origin, Professional History.
ACCESS CONTROL DATA	Personal Data is collected via email and/or other tools directly by Seaborn for physical and/or logical access control purposes.	Customer Visitor Vendor	Name, E-mail, Tax ID (e.g., CPF), Government-issued ID (e.g., CNH, Driver's License and/or Passport), License Plate, Security Camera Videos and Images.
AUTOMATICALLY COLLECTED DATA	Personal Data is collected when the Data Subject accesses Seaborn's platforms and/or website.	User	Cookies, IP Address, Date, and Time of Visit.

REQUEST DATA	Personal Data is collected when the Data Subject makes a request related to Personal Data through official communication channels.	All Data Subjects, including Former Employees	Name, E-mail, Date of Birth, Mother's Name, Tax ID (e.g., CPF).

5.2 In addition to the types of Personal Data expressly listed above, we may request that you provide us other Personal Data as necessary to achieve any lawful purpose provided that such request complies with applicable DPP Law.

5.3 You are responsible for informing us immediately of any changes or corrections to your Personal Data to ensure that your Personal Data is accurate and up to date.

6. Why Do We Process Personal Data?

6.1 We collect, maintain, and Process Personal Data that is required as part of our business operations in compliance with applicable DPP Law. We Process Personal Data to pursue the legitimate business interests, listed in the chart below. The chart also lists the applicable Legal Basis for each purpose and the Personal Data groups involved in each processing activity. Where the applicable Legal Basis is the legitimate interest of the Controller, the purpose and description also describe our legitimate interest in processing Personal Data.

PURPOSE & LEGAL BASIS FOR COLLECTING PERSONAL DATA			
PURPOSE	**DESCRIPTION**	**DATA GROUP**	**LEGAL BASIS**
Customer Acquisition and Prospecting	Conduct procedures related to sales and contract prospecting with Seaborn, such as acquisition, negotiation, contact, offering, and other preliminary and necessary actions for contract execution.	• Contact Data	• Legitimate Interest of the Controller
Vendor Selection and Management	Conduct procedures related to vetting and retaining Vendors, such as acquisition, negotiation, contact, offering, and other preliminary and necessary actions for contract execution	• Contact Data • Contract Data	• Legitimate Interest of the Controller
Performance and Fulfillment of Contracts	Enter into and manage contracts signed by Seaborn, including contract management, payment execution, delivery of contracted services to Customers.	• Contract Data	• Legitimate Interest of the Controller (legal entity representatives) • Execution of Contract or Preliminary Procedures
Promotion and Advertising of Services Provided by Seaborn	Carry out promotional activities through Seaborn's communication channels with the general public to provide information about the services offered.	• Advertising Data • Automatically Collected Data	• Legitimate Interest of the Controller • Consent

PURPOSE & LEGAL BASIS FOR COLLECTING PERSONAL DATA			
PURPOSE	**DESCRIPTION**	**DATA GROUP**	**LEGAL BASIS**
Collection of Payments and Other Unfulfilled Obligations	Collect overdue payments from Customers and/or enforce other unfulfilled obligations by Customers.	• Contract Data	• Regular exercise of rights in judicial, administrative, or arbitration procedures (Brazil Data Subjects only) • Legitimate Interest of the Controller (Other Data Subjects only)
Compliance Obligations and Audits	Perform audit procedures and other processes for internal and/or external compliance purposes.	• All Data	• Legitimate Interest of the Controller • Regular exercise of rights in judicial, administrative, or arbitration procedures (Brazil Data Subjects only, Sensitive Personal Data)
Credit Risk Check	Conduct prior analysis of the hiring company's profile to evaluate credit risk.	• Contact Data	• Protection of Credit (Brazil Data Subjects only) • Legitimate Interest of the Controller (Other Data Subjects only)
Recruitment of New Employees	Conduct selection processes for Potential Employees to hire new staff for Seaborn.	• Candidate Data	• Legitimate Interest of the Controller
Legal and Administrative Compliance	Carry out necessary processes to ensure Seaborn's compliance with applicable legal obligations. These processes include, for example, contract management, internal compliance obligations, and analysis of legal proceedings, among others.	• Contract Data • Candidate Data	• Compliance with a legal or regulatory obligation
Defense of Seaborn's Rights and Interests	Defend Seaborn's interests and rights in administrative, arbitral, or judicial proceedings, as well as in extrajudicial or pre-litigation negotiations, such as mediation, conciliation, or out-of-court settlements.	• All Data	• Regular exercise of rights in judicial, administrative, or arbitration procedures (Brazil Data Subjects only) • Legitimate Interests of the Controller (Other Data Subjects only)
Control and Management of Access to Physical Premises & Logical Systems	Grant, monitor, maintain, and revoke access for individuals who, in any way, interact with Seaborn's premises and physical assets, including personal and/or vehicular access.	• Access Control Data	• Legitimate Interest of the Controller
Use of Website	Allow access to and use of Seaborn's website.	• Automatically Collected Data	• Legitimate Interest of the Controller
Response to Data Subjects' Requests	Analyze, respond to, monitor, and/or address Data Subject requests to exercise rights under the Brazil LGPD, particularly those in Article	• Request Data	• Compliance with a legal or regulatory obligation

PURPOSE & LEGAL BASIS FOR COLLECTING PERSONAL DATA			
PURPOSE	**DESCRIPTION**	**DATA GROUP**	**LEGAL BASIS**
	18 of the Brazil LGPD or other applicable DPP Law.		
Fraud Prevention	Investigate, prevent, or take measures related to illegal activities, suspected fraud, or situations involving potential threats to the physical security of individuals, partner companies, Seaborn, or as otherwise legally required within the limits permitted by applicable DPP Law.	• All Data	• Legitimate Interest of the Controller • Fraud prevention and the Data Subject's safety (Brazil Data Subjects only)
Corporate Transactions	Carry out merger, acquisition, restructuring, or incorporation operations.	• All Data	• Legitimate Interest of the Controller • Regular exercise of rights in judicial, administrative, or arbitration procedures (Brazil Data Subjects only, Sensitive Personal Data)
Legal Obligations	Fulfill legal and/or regulatory obligations with competent authorities, which may include maintaining tax and labor records, website access logs, and others, as well as disclosing certain data or performing certain acts before public authorities, such as mandatory registrations, obtaining licenses, and authorizations, among others.	• All Data	• Compliance with a legal or regulatory obligation

7. Sharing Personal Data

7.1 We may share your Personal Data with the following recipients in order to achieve our purpose listed in the previous section:

a) Legal entities that are part of the Seaborn economic group, when necessary for the regular provision of Seaborn's services; provided, however, that with respect to Brazil Data Subjects we do so in compliance with our obligations under the ITDA as defined and described in Section 8 below;

b) Commercial partners and service providers, when necessary to enable the services provided by Seaborn, such as (i) infrastructure and technology required for a Platform's operational performance, (ii) cloud computing, (iii) data backup, (iv) invoice issuance, (v) billing services, and (vi) organization of events, fairs, and workshops, and to promote and advertise the services provided by Seaborn;

c) Public agencies, competent authorities, and insurers, when necessary for compliance with legal and/or regulatory obligations or for the regular exercise of Seaborn's rights in arbitration, administrative, or judicial proceedings; and

d) Legal entities involved in corporate operations that entail the restructuring of the business group to which Seaborn belongs, when necessary to facilitate the corporate operation in question in which Seaborn and its assets are involved.

7.2 In the event we enter into third-party contracts with Processors or Controllers, including renewal of agreements now in place, we will use our reasonable efforts to ensure that they have an appropriate legal and organizational structure for Processing your Personal Data.

8. International Data Transfers

8.1 Seaborn transfers data between and among our affiliates in the United States and Brazil, as well as to the third parties described in Section 7. California Data Subject and Other Data Subject Personal Data is primarily stored in the United States and Brazil Data Subject Personal Data is primarily stored in Brazil, but it may also be stored in, or stored on IT equipment located in other countries. As a result, your Personal Data may be processed in a foreign country where privacy laws may be less stringent than the laws in your country. Whenever we transfer Personal Data originating in one country to one of our affiliates or a third party in a different country, we will implement appropriate safeguards, consistent with applicable DPP Law of the country from which the Personal Data is exported, including with respect to data transfers between and among our affiliates in the United States and Brazil, in compliance with the International Data Transfer Agreement ("**IDTA**") described in Section 8.3.

8.2 Seabras Brasil may transfer the Personal Data of Brazil Data Subjects to locations outside Brazil as part of its business operations provided that any such international data transfer is supported by the contractual instruments with the recipient party(ies) required by the Brazil LGPD, including adoption of the standard contractual clauses mandated by the Regulation on International Transfer of Personal Data (Resolution CD/ANPD Nº 19, of August 23, 2024) of the Brazil ANPD, and related Brazil ANPD regulations and/or guidelines.

8.3 Seabras Brasil confirms that the IDTA it has entered into with its affiliates complies with the requirements set forth in Section 8.1. In addition, we provide you key information regarding the international data transfer arrangement under the IDTA in attached ***Annex A-1*** in accordance with the provisions of Annex II, Clause 14.1 of Resolution CD/ANPD No. 19.

9. Security & Storage or Personal Data

9.1 Seaborn employs reasonable efforts to ensure the security of the Systems we use in the Processing of your Personal Data, including:

a) Adoption of Seaborn's Information Security Policy, that establishes technical, physical, and administrative measures to keep Personal Data secure and protected against unauthorized access, accidental or unlawful destruction, loss, alteration, communication, or any other inappropriate or illegal

Processing, as may be required under applicable DPP Law, including data encryption according to market best practices;

b) Maintaining all information confidential and granting access only to those individuals responsible for ensuring its proper use; and

c) Raising awareness among our employees about best practices in data privacy and protection in accordance with applicable DPP Law.

9.2 The Platform may contain links redirecting you to other third-party pages which may have different policies from those outlined in this document. We are not responsible for the collection, use, sharing, or storage of information and/or Personal Data by the entities responsible for such pages outside Seaborn's domain.

9.3 The Personal Data we collect from you will be stored in secure physical locations or on proprietary or contracted Systems, located nationally or internationally, for a defined period in order to:

a) Comply with applicable hold period(s) required by laws, resolutions, and/or other regulations;

b) achieve the designated purpose for the Personal Data Processing, including the purposes described in Section 6;

c) preserve Seaborn's legitimate interests, as applicable; and/or

d) safeguard our regular exercise of rights in judicial, administrative, or arbitration proceedings, including in compliance with applicable prescription periods.

9.4 Except as permitted or required by applicable law, your Personal Data will be deleted when:

a) the Processing purpose is achieved;

b) the Personal Data is no longer necessary or relevant to achieve the specific intended purpose;

c) you exercise your right to withdraw Consent, if required under applicable DPP Law; or

d) as determined by any applicable government agency or authority over this data protection issue, including the Brazil ANPD in cases of Brazil LGPD violations.

10. What Are Your Rights & How Can You Exercise

10.1 As a Data Subject you may have the following rights under applicable DPP Law, subject to certain limitations. If you are a Brazil Data Subject, the rights applicable to you are listed in ***Annex A***. If you are a California Data Subject, the rights applicable to you are listed in ***Annex B***.

a) Access to Personal Data: request access to your Personal Data that we have Processed. We cannot disclose to you any Personal Data other than your Personal Data.

b) Correction or Update of Personal Data: request we correct or update your Personal Data if it is inaccurate, incomplete, or outdated.

c) Portability of Personal Data: request a copy of your Personal Data collected by Seaborn for transfer to another organization, provided such requested transfer is compliant with applicable DPP Law.

d) Deletion of Personal Data: request the deletion of your Personal Data Processed by us. Your Personal Data will not be deleted in cases where retention is authorized by applicable DPP Law or otherwise required by applicable law.

e) Restriction of Personal Data: request that we restrict our Processing of your Personal Data under certain circumstances.

f) Withdrawal of Consent: withdraw your Consent for our Processing your Personal Data for certain purposes at any time. It is important to note that withdrawing your Consent does not result in the deletion of Personal Data that we lawfully retain on a different Legal Basis.

g) Objection to Processing: object to our Processing your Personal Data, depending on our Legal Basis for that Processing.

h) Reporting to Your Local Supervisory Authority: report any incident related to your Personal Data to your local supervisory authority**.**

10.2 To exercise the rights described in Section 10.1, you may submit a request to us by using our online form available at https://seabornnetworks.com/formexternalprivacypolicy or emailing us at USDPO@seabornnetworks.com. To ensure the security of Personal Data when responding to requests, we may request information and documents to verify the identity and authenticity of the requesting Data Subject.

11. Contact Information

11.1 For questions, complaints, or any need for communication regarding your Personal Data protection in Brazil under this External Privacy Policy, you can contact Seabras Brasil's Brazil Data Protection Officer. Her contact details are:

Brazil Data Protection Officer: Maria Beatriz M. de Miranda Tello
Email: BrasilDPO@seabornnetworks.com

11.2 For questions, complaints, or any need for communication regarding your Personal Data protection outside Brazil under this External Privacy Policy, you can contact our Global Data Protection Officer. Her contact details are:

Global Data Protection Officer: Lin Gentemann
Email: USDPO@seabornnetworks.com

11.3 Contact details for Seaborn's UK representative are:

Rickert Services Ltd UK
- Seabras 1 USA, LLC -
PO Box 1487
Peterborough

PE1 9XX
United Kingdom
art-27-rep-Seabras 1 USA, LLC@rickert-services.uk

11.4 Contact details for Seaborn's EU representative are:

Rickert Rechtsanwaltsgesellschaft mbH
- Seabras 1 USA, LLC -
Colmantstraße 15
53115 Bonn
Germany
art-27-rep-Seabras 1 USA, LLC@rickert.law

12. General Provisions

12.1 This External Privacy Policy may be modified by Seaborn at any time. To check the current version of the External Privacy Policy at the time of your inquiry, verify the information in the footer of this External Privacy Policy.

12.2 If we make any substantial changes to this External Privacy Policy, you will be informed of these changes by accessing our website, where the updated version will be published with appropriate notification.

12.3 By continuing to access or use our services after the effective date of such changes, you accept and agree to be bound by the revised version of this External Privacy Policy.

12.4 This External Privacy Policy shall be governed and interpreted as follows unless otherwise expressly required by law:

a) with respect to Brazil Data Subjects, the laws of the Federative Republic of Brazil; and

b) with respect to California Data Subjects and Other Data Subjects, the laws of the Commonwealth of Massachusetts, USA.

12.5 The jurisdiction and forum for resolving any disputes regarding the interpretation and enforcement of this External Privacy Policy will be as follows unless otherwise expressly required by law:

a) with respect to Brazil Data Subjects, you and we elect the exclusive jurisdiction and forum of the courts sitting in the district of São Paulo, state of São Paulo, Brazil; and

b) with respect to California Data Subjects and Other Data Subjects, you and we elect the exclusive jurisdiction and forum of the state and federal courts sitting in Boston, Massachusetts.

However, before initiating formal legal proceedings, you are encouraged to contact a DPO listed in Section 11 above to resolve your concerns directly.

12.6 If any provision of this External Privacy Policy is found invalid, illegal, or unenforceable in any respect, the validity, legality, or enforceability of the remaining provisions will not be affected or impaired as a result.

12.7 This External Privacy Policy is effective on the date of its publication.

ANNEX A: BRAZIL DATA SUBJECT RIGHTS

This ***Annex A*** describes the rights of Brazil Data Subjects and key terms of Seaborn's international data transfer agreement as required under the Brazil LGPD.

The Brazil LGPD establishes certain specific rights for Brazil Data Subjects, including the right to:

a) Confirmation of Processing: request our confirmation that we are Processing your Personal Data.

b) Access to Personal Data: request access to your Personal Data that we have Processed. We will provide you a copy of stored Personal Data through electronic or physical means. We cannot disclose to you any Personal Data other than your Personal Data.

c) Correction or Update of Personal Data: request we correct or update your Personal Data if it is inaccurate, incomplete, or outdated. Before updating, we may request supporting documents and/or information from you to verify the details provided to us**.**

d) Anonymization, Blocking, or Deletion of Personal Data: request that your unnecessary, excessive, or noncompliant Personal Data be Anonymized, blocked, or deleted from our database.

e) Portability of Personal Data: request the transfer of your Personal Data collected by Seaborn to another organization, provided such requested transfer is compliant with the Brazil ANPD regulations**.**

f) Deletion of Personal Data: request the deletion of your Personal Data Processed by us based on your Consent at any time through a free and facilitated process. Your Personal Data will not be deleted in cases where retention is authorized by the Brazil LGPD or otherwise required by law**.**

g) Information About Data Sharing: request information regarding our sharing of your Personal Data with third parties.

h) Information About the Possibility of Denying Consent: request information regarding your option to deny us Consent to Process your Personal Data. Upon our receipt of such request, we will communicate to you the consequences of denying us your Consent, which, in some situations, may prevent our provision of certain services to you**.**

i) Withdrawal of Consent: withdraw your Consent for our Processing your Personal Data for certain purposes at any time. It is important to note that withdrawing your Consent does not result in the deletion of Personal Data that we lawfully retain on a different Legal Basis.

j) Objection to Processing: object to our Processing your Personal Data if our Legal Basis for waiving Consent that does not comply with the Brazil LGPD.

k) Reporting to the Brazil ANPD and Consumer Protection Agencies: report any incident related to your Personal Data to the Brazil ANPD and/or a Brazilian consumer protection agency**.**

l) Review of Automated Decision-Making and Explanation: request that we review a decision that was based solely on automated Processing of Personal Data that affect your interests, including decisions intended to define your personal, professional, consumer, or credit profile, or aspects of your personality. You may also request clear and adequate information about the criteria and procedures used for automated

decisions, provided such request complies with applicable requirements regarding trade and industrial secrets**.**

To exercise the rights described in this ***Annex A***, you may submit a request to us by using our online form available at https://seabornnetworks.com/formexternalprivacypolicy, or emailing us at BrasilDPO@seabornnetworks.com. To ensure the security of Personal Data when responding to requests under this ***Annex A***, we may request information and documents to verify the identity and authenticity of the requesting Data Subject. Seabras Brasil, through the office of the Brazil DPO, will respond to any such request in accordance with the Brazil LGPD, including applicable response times.

ANNEX A-1: INTERNATIONAL DATA TRANSFER AGREEMENT KEY TERMS

Key Terms of Seaborn's International Data Transfer Agreement	
INFORMATION	**DESCRIPTION**
Form	The international data transfers are based on the Standard Contractual Clauses mandated under Annex II of Resolution CD/ANPD Nº 19.
Duration	Storage will be maintained for the period permitted by law and in accordance with Seaborn's internal retention and disposal policies.
Purpose of the international transfer	• Enable Seabras 1 Brasil Ltda. to provide access to Seabras 1 USA, LLC and its affiliates for the Processing of Brazil Data Subject's Personal Data collected by Seabras 1 Brasil Ltda. • Enable the use of third-party software, as described below.
Destination country of the transferred data	United States of America and member countries of the European Union.
Identification and Contact Details of Controller	• **Seabras 1 Brasil Ltda.**, registered under CNPJ No. 17.289.520/0001-69, headquartered at Av. Paulista, No. 352, 7th Floor, Suite 77, ZIP Code 01.310-905, Bela Vista, São Paulo (Controller). • **Seabras 1 USA, LLC**, a limited liability company duly organized and existing under the laws of the State of Delaware, with its principal place of business at 600 Cummings Center, Suite 268Z, Beverly, MA 01915, United States, the parenting company of Seaborn.
Shared use of data by the Parties	**Personal Data Shared:** • Recruitment and Selection Data • Contract Management Data • Candidate Data • Access Control Data • Occupational Health Data • Benefits Management Data • Termination Management Data • Expenses and Travel Data • Access Registration Data in IT Systems • Data for Supplier Approval • Financial Reporting Data • Request Data • Legal and Corporate Management Data • Investigation and Discipline Data
Purposes of Data Processing by Importers	**Purposes for Data Processing:** • Manage Financial Operations • Administer Legal, Compliance, and Contractual Matters • Oversee External Relationships • Direct Human Resources and Internal Governance • Manage IT and Operational Processes • Drive Sales and Marketing Initiatives • Ensure Information and Endpoint Security (e.g., Sophos)

	• Facilitate Business Productivity and Communication (e.g., Microsoft 365) • Manage Employee Expenses (e.g., Expensify) • Enable Cloud File Storage and Collaboration (e.g., Dropbox) • Support Accounting and Tax Compliance in Brazil (e.g., Contmatic) • Manage Human Resources and Employee Time Tracking (e.g., Tangerino)
Responsibilities of the agents who shall conduct the processing	Seabras 1 Brasil Ltda. is responsible for publishing information regarding the international data transfer, for receiving and handling data subject requests, for reporting security incidents to the Brazil ANPD, among other duties.
Security Measures Adopted	Seaborn has adopted policies, including an Information Security Policy, establishing Security Measures to protect Personal Data, including: • Administrative Controls, such as internal policies, processes, and guidelines governing the security controls for the processing of personal data; internal policies, processes, and guidelines regarding the handling of and response to security incidents; internal policies, processes, and guidelines concerning the information security program adopted by Seaborn, among others. • Technical Controls, such as Identity and Access Management (IAM); Role-based access control (RBAC); Geolocation "IP fence"; Network IP ACL (access control lists); Multi-Factor Authentication (MFA)/2FA; Endpoint and Device Security; MDR filtering; Encryption, including encryption in transit using SSL/HTTPS and encryption at rest, among others. • Physical Controls, such as Access Controls Systems; Video Surveillance Systems (CCTV); among others.
Data Subject's rights and the means for exercising them	This information is thoroughly described in Sections 10 and 12 of Seaborn's External Privacy Policy (Version 1.0).

ANNEX B: CALIFORNIA DATA SUBJECT RIGHTS

This ***Annex B*** describes the rights of California Data Subjects under the CCPA and provides certain information as required under the CCPA.

Your Personal Data

We may collect some or all of the following categories of Personal Data from or about you for the following purposes:

DATA CATEGORY	DATA ELEMENTS	PURPOSE
IDENTIFIERS	Name, Email, Phone Number, Address, Government issued-ID, IP Address, License Plate	Customer acquisition and prospecting, credit risk check, performance and fulfillment of contract, collection of payments and other unfulfilled obligations, legal and administrative compliance, promotion and advertising of services provided by Seaborn, vendor selection and management, recruitment of new employees, control and management of access to physical premises and logical systems (Visitors, Vendors, Customers), use of website, response to data subjects' requests
PERSONAL INFORMATION DESCRIBED IN CAL. CIV. CODE § 1798.80(E)	Name, Email, Phone Number, Address, Government-issued ID, IP Address, License Plate, Signature, Picture, Employer (Name of the Company), Title (Job Position), Professional History	
CHARACTERISTICS OF PROTECTED CLASSIFICATION UNDER CALIFORNIA OR FEDERAL LAW	Country of Origin, Age, Date of Birth,	Legal and administrative compliance, recruitment of new employees, vendor selection and management, control and management of access to physical premises and logical systems, response to data subjects' requests
PROFESSIONAL OR EMPLOYMENT-RELATED INFORMATION	Employer (Name of the Company), Title (Job Position), Professional History	Customer acquisition and prospecting, credit risk check, performance and fulfillment of contracts, collection of payments and other unfulfilled obligations, legal and administrative compliance, vendor selection and management, recruitment of new employees, control and management of access to physical premises and logical systems
INTERNET OR OTHER ELECTRONIC NETWORK ACTIVITY INFORMATION	Cookies, IP Address, Address, Date, and Time of Visit	Customer acquisition and prospecting, performance and fulfillment of contracts, collection of payments and other unfulfilled obligations, legal and administrative compliance, promotion and advertising of services provided by Seaborn, use of website

DATA CATEGORY	DATA ELEMENTS	PURPOSE
VISUAL INFORMATION	Security Camera Videos and Images	Control and management of access to physical premises and logical systems (Visitors, Vendors)
SENSITIVE PERSONAL INFORMATION: SOCIAL SECURITY NUMBER, DRIVER'S LICENSE, STATE ID CARD, OR PASSPORT NUMBER	Driver's License, State ID, or Passport	Legal and administrative compliance, vendor selection and management, control and management of access to physical premises and logical systems
SENSITIVE PERSONAL INFORMATION: CITIZENSHIP OR IMMIGRATION STATUS	Passport	Legal and administrative compliance, vendor selection and management control and management of access to physical premises and logical systems
ALL DATA CATEGORIES LISTED ABOVE		Compliance and audit obligations, defense of Seaborn's rights and interests, fraud prevention, corporate transactions, legal obligations

For a description of the sources of this Personal Data, see Section 4 (How Is Personal Data Collected). For a detailed description of the listed purposes, see Section 5 (Why Do We Process Personal Data?). For a description of the third parties to which we disclose these categories of Personal Data and the purposes of those disclosures, see Section 7 (Sharing Personal Data).

Seaborn does not sell Personal Data in the conventional sense (i.e., for money). Like many companies, however, we use third-party ad serving and measurement providers that help us advertise our services online and measure the performance of those ads. Through the use of cookies and related technologies, we may collect and transfer Personal Data related to your interactions with our website (specifically, internet activity information and related identifiers) to these providers for their use. Making Personal Data available to these providers may be considered a "sale or "sharing" of your Personal Data under the CCPA. We do not knowingly sell or share the Personal Data of individuals under the age of 16.

Your Privacy Rights

California residents have the following rights, subject to certain limitations:

1. **Right to know**. You have the right to request that we disclose the following information to you about our collection and use of your Personal Data over the past 12 months: (1) the categories of Personal Data we collected about you; (2) the categories of sources for the Personal Data we collected about you; (3) our business or commercial purpose for collecting, selling, or sharing that Personal Data; (4) the categories of third parties to whom we disclose that Personal Data; (5) a list of categories of Personal Data disclosed for a business purpose and the categories of recipients; (6) a list of categories

of Personal Data sold and/or shared and the categories of recipients; and (7) and the specific pieces of Personal Data we have collected about you.

2. **Right to correct**. You have the right to correct inaccurate Personal Data maintained by us.
3. **Right to delete**. You have the right to request that we delete Personal Data we collected from you, subject to certain exceptions. In many situations we must keep your Personal Data to comply with our legal obligations, resolve disputes, enforce our agreements, or for another one of our business purposes.
4. **Right to opt out of sale or sharing.** You have the right to opt out of the sale or sharing of Personal Data. You can opt out of the sale or sharing of Personal Data by clicking here https://seabornnetworks.com/formexternalprivacypolicy
5. **Right not to be discriminated or retaliated against.** We do not discriminate or retaliate against you in any manner prohibited by applicable law for exercising your rights.

To exercise the rights to know, correct, and delete, please submit a request to us by using our online form available at https://seabornnetworks.com/formexternalprivacypolicy, emailing us at USDPO@seabornnetworks.com, or calling us at 1-888 224 0268. Please explain your request clearly and with enough detail so that we can understand it and respond to it properly.

Under certain circumstances, California Data Subjects can limit use and disclosure of their Sensitive Personal Data to certain purposes specified by law (e.g., providing you with services you request or preventing security incidents). We only use Sensitive Personal Data for such permitted purposes and do not disclose Sensitive Personal Data, so we don't offer the opportunity to limit the use and disclosure of your Sensitive Personal Data.

We may need to confirm who you are before we can help with your request. This is to make sure that your request is related to your Personal Data. Depending on your request, we may ask you for some information that you've already given us, such as your name, address, username, or email address, to confirm your identity. We may also ask you to sign a statement confirming your identity.

You may also appoint an authorized agent to submit requests to exercise certain privacy rights on your behalf. We will require verification that you provided the authorized agent permission to make a request on your behalf. You must provide us with a copy of the signed permission you have given to the authorized agent to submit the request on your behalf and verify your identity directly with us.