



Privacy Policy



.....	1
1. Introduction	1
1.1 Purpose of this Privacy Policy	1
1.2 Scope of Application	1
1.3 Relationship with the Terms of Use	2
1.4 Acceptance and Acknowledgement	2
2. Data Controller and Contact Information	3
2.1 Data Controller.....	3
2.2 Contact Details	3
2.3 Privacy and Data Protection Enquiries.....	4
3. Personal Data We Collect	4
3.1 Identity Information	4
3.2 Contact Information	5
3.3 Account and Authentication Information	5
3.4 Company and Professional Information	5
3.5 Vessel and Maritime Information	6
3.6 Application, Survey and Certification Information	6
3.7 Documents and Uploaded Content	6
3.8 Communications and Correspondence	7
3.9 Technical, Device and Usage Information	7
3.10 Log, Security and Audit Information.....	7
3.11 Information Received from Third Parties	8
4. How We Collect Personal Data.....	8
4.1 Information Provided Directly by You	8
4.2 Information Provided by Your Organisation.....	9

4.3 Information Generated Through Use of the Platform	9
4.4 Information Obtained from Public and Official Sources	10
4.5 Information Received from Third Parties and Service Providers.....	10
5. Purposes of Processing Personal Data	10
5.1 Account Creation and Administration	11
5.2 Company and User Verification	11
5.3 Vessel Registration and Management	11
5.4 Classification and Certification Services.....	12
5.5 Survey, Audit and Inspection Activities.....	12
5.6 Application and Request Management	13
5.7 Communications and Notifications.....	13
5.8 Document and Certificate Management	13
5.9 Platform Security and Fraud Prevention	14
5.10 Legal and Regulatory Compliance	14
5.11 Service Improvement and Analytics	14
5.12 Establishment, Exercise and Defence of Legal Claims	15
6. Legal Bases for Processing.....	15
6.1 Performance of a Contract	16
6.2 Compliance with Legal Obligations	16
6.3 Legitimate Interests	16
6.4 Consent	17
6.5 Protection of Vital Interests	17
6.6 Other Applicable Legal Bases	17
7. Special Categories and Sensitive Information	18
7.1 Special Categories of Personal Data	18
7.2 Identification and Official Documents	19
7.3 Processing Restrictions and Safeguards.....	19
8. Sharing and Disclosure of Personal Data	20
8.1 Flag Administrations and Maritime Authorities	20
8.2 Port State and Other Competent Authorities.....	20
8.3 Recognized Organisations and Classification Societies.....	21

8.4 Surveyors, Auditors and Authorized Personnel	21
8.5 Vessel Owners, Managers and Other Authorized Organisations	21
8.6 Service Providers and Technology Partners	22
8.7 Professional and Legal Advisers	22
8.8 Disclosure Required by Law	22
8.9 Corporate Transactions and Organisational Changes	23
9. International Transfers of Personal Data.....	23
9.1 International Nature of LSR Services	23
9.2 Transfers Outside the Country of Collection	24
9.3 Transfer Safeguards.....	24
9.4 Transfers to Maritime Authorities and Organisations	25
10. Data Retention.....	25
10.1 General Retention Principles	26
10.2 Account and User Records	26
10.3 Vessel, Survey and Certification Records	26
10.4 Communications and Operational Records	27
10.5 Security and Audit Logs	27
10.6 Legal and Regulatory Retention Requirements	27
10.7 Deletion, Anonymisation and Archiving	28
11. Data Security.....	28
11.1 Technical and Organisational Measures	29
11.2 Access Controls and Authorization	29
11.3 Authentication and Account Security	29
11.4 Document and Data Protection	30
11.5 Monitoring and Audit Trails	30
11.6 Personal Data Breach Management.....	31
12. Cookies, Analytics and Similar Technologies	31
12.1 Cookies and Local Storage	32
12.2 Essential Technologies.....	32
12.3 Analytics and Performance Technologies	33
12.4 Security and Fraud-Prevention Technologies	33

12.5 Cookie Preferences and Controls.....	33
13. Automated Processing and Artificial Intelligence	34
13.1 Automated Processing	34
13.2 Risk, Security and Fraud Detection.....	35
13.3 Artificial Intelligence-Assisted Features	35
13.4 Human Review and Decision-Making.....	36
14. Your Privacy Rights	36
14.1 Right of Access	37
14.2 Right to Rectification.....	37
14.3 Right to Erasure	37
14.4 Right to Restriction of Processing.....	38
14.5 Right to Data Portability.....	38
14.6 Right to Object	39
14.7 Rights Relating to Automated Decision-Making	39
14.8 Withdrawal of Consent.....	39
14.9 Right to Lodge a Complaint	40
14.10 Exercising Your Rights	40
15. Third-Party Services and External Links	40
15.1 Third-Party Platforms and Services	41
15.2 External Websites and Links	41
15.3 Third-Party Privacy Practices	42
16. Children's Privacy.....	42
16.1 Age Restrictions.....	42
16.2 Unintentional Collection of Children's Data	43
17. Changes to this Privacy Policy.....	43
17.1 Policy Updates.....	44
17.2 Material Changes.....	44
17.3 Effective Date and Version History	45
18. Contact Us	45
18.1 Privacy Enquiries	45
18.2 Data Protection Requests.....	46

18.3 Complaints and Regulatory Matters	46
<i>Appendix A — Categories of Personal Data and Processing Purposes.....</i>	47
<i>Appendix B — Data Retention Framework</i>	61
<i>Appendix C — Categories of Recipients.....</i>	71
<i>Appendix D — International Data Transfer Framework</i>	78
<i>Appendix E — Privacy Policy Version History</i>	85

1. Introduction

1.1 Purpose of this Privacy Policy

This Privacy Policy explains how Life At Sea Register ("LSR") collects, uses, processes, stores, protects, shares, and otherwise handles personal data in connection with the use of the LSR Client Portal (the "Portal") and the services provided through or in connection with the Portal.

The purpose of this Privacy Policy is to provide users, representatives of client organizations, surveyors, auditors, applicants, and other individuals whose personal data may be processed by LSR with clear and transparent information regarding the processing of their personal data.

This Privacy Policy describes the categories of personal data that may be collected, the purposes and legal bases for processing, the circumstances in which personal data may be shared with third parties or competent authorities, applicable international data transfers, data retention and security practices, and the rights available to individuals under applicable data protection laws.

LSR processes personal data only where there is an appropriate purpose and legal basis for doing so and seeks to apply principles of lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality in its processing activities.

This Privacy Policy should be read together with the LSR Client Portal Terms of Use and any additional privacy notices, consent statements, contractual provisions, or other information provided in connection with a particular LSR service or processing activity.

1.2 Scope of Application

This Privacy Policy applies to personal data processed by Life At Sea Register ("LSR") in connection with the LSR Client Portal (the "Portal") and the services, activities, communications, and processes carried out through or in connection with the Portal.

This Privacy Policy applies to individuals whose personal data may be processed by LSR, including Portal users, applicants, authorized representatives of shipowners, managers, operators and other organizations, company administrators, surveyors, auditors, consultants, contractors, and other persons involved in services or activities administered through the Portal.

The Policy covers personal data provided directly by individuals, submitted by organizations or authorized representatives, obtained from competent authorities or other legitimate sources, and generated or recorded through the use and operation of the Portal.

It applies to personal data processed in connection with account administration, company and vessel management, applications, surveys, audits, inspections, technical reviews, classification and certification activities, document management, communications, security, compliance, and other services or functions provided by LSR through or in connection with the Portal.

Where a specific service, processing activity, contractual arrangement, or legal requirement is subject to an additional privacy notice or specific data protection provisions, such provisions shall apply together with this Privacy Policy and shall supplement it in relation to the relevant processing activity.

1.3 Relationship with the Terms of Use

This Privacy Policy forms part of the legal and operational framework governing the use of the LSR Client Portal and should be read together with the LSR Client Portal Terms of Use ("Terms of Use").

The Terms of Use govern access to and use of the Portal, including user responsibilities, account security, acceptable use, confidentiality, document handling, electronic records, and other conditions applicable to Portal users. This Privacy Policy specifically explains how personal data is collected, processed, stored, protected, transferred, shared, and otherwise handled by LSR.

References to privacy, personal data, monitoring, audit records, security information, or data retention within the Terms of Use should therefore be understood together with the more detailed provisions contained in this Privacy Policy.

In the event of any inconsistency between the Terms of Use and this Privacy Policy concerning the processing or protection of personal data, this Privacy Policy shall prevail in relation to that matter, unless otherwise required by applicable law or a specific legally binding arrangement.

Nothing in this Privacy Policy modifies or limits any other contractual, statutory, regulatory, classification, certification, or professional obligation applicable to LSR, a user, or an organization using the Portal.

1.4 Acceptance and Acknowledgement

By accessing or using the Portal, users acknowledge that they have been provided with access to this Privacy Policy and have had the opportunity to review information regarding how LSR processes personal data in connection with the Portal and its related services.

Acknowledgement of this Privacy Policy does not, by itself, constitute consent to every processing activity described herein. Where consent is required as the legal basis for a specific processing activity, LSR will seek such consent separately and in an appropriate manner.

Certain processing activities may be necessary for the performance of a contract, compliance with legal or regulatory obligations, protection of legitimate interests, operation and security of the Portal, classification or certification activities, or other lawful purposes and may therefore be carried out without relying upon consent where permitted by applicable law.

Users acting on behalf of an organization are responsible for ensuring that personal data relating to other individuals is submitted to LSR lawfully and that such individuals are provided with any information or notices required under applicable data protection laws.

Continued use of the Portal following an update to this Privacy Policy constitutes acknowledgement of the updated Policy. Where applicable law requires specific notice, consent, or another action in relation to a material change, LSR will take the measures required before the relevant processing is undertaken.

2. Data Controller and Contact Information

2.1 Data Controller

Life At Sea Register ("LSR") is responsible for the processing of personal data for which it determines the purposes and means of processing in connection with the LSR Client Portal (the "Portal") and the services provided by LSR.

Depending on the nature of the relevant service, relationship, and processing activity, LSR may process personal data in connection with user account administration, company and vessel management, applications, surveys, audits, inspections, technical reviews, classification and certification activities, communications, document management, security, compliance, and other operational activities.

In certain circumstances, personal data processed through the Portal may have been provided by or relate to a shipowner, manager, operator, employer, flag administration, competent authority, recognized organization, service provider, or other third party. The respective responsibilities of LSR and such parties for the processing of personal data shall be determined according to the nature of the processing activity, the applicable contractual arrangements, and applicable data protection law.

Where LSR processes personal data on behalf of another organization and does not determine the purposes and means of that processing, its role and obligations shall be governed by the applicable contractual arrangements and data protection requirements.

Nothing in this Privacy Policy is intended to alter the legal status or responsibilities of any party where such status or responsibilities are determined by applicable data protection law.

2.2 Contact Details

Questions, requests, or communications concerning this Privacy Policy or the processing of personal data by Life At Sea Register may be submitted through the official contact channels designated by LSR.

Life At Sea Register (LSR)

Website: www.lsregister.com

Email: support@lsregister.com

Current contact information and any additional communication channels designated for privacy or data protection matters may be published through the official LSR website or the Portal.

Users and other individuals submitting privacy-related communications are responsible for using the current contact information made available by LSR.

LSR may request reasonable information necessary to verify the identity or authority of a person making a request before disclosing personal data or taking action in relation to that request.

2.3 Privacy and Data Protection Enquiries

Individuals may contact LSR regarding questions, concerns, or requests relating to this Privacy Policy, the processing of their personal data, or the exercise of rights available under applicable data protection laws.

Privacy and data protection enquiries may include requests concerning access to personal data, correction of inaccurate information, deletion or restriction of processing, data portability, objections to processing, withdrawal of consent where applicable, or information regarding the manner in which personal data is processed.

Requests should contain sufficient information to enable LSR to understand and appropriately respond to the matter. LSR may request additional information where reasonably necessary to verify the identity of the requester, confirm their authority to act on behalf of another person, locate the relevant records, or prevent unauthorized disclosure of personal data.

LSR will review and respond to valid privacy and data protection requests in accordance with applicable legal requirements and within any time limits prescribed by applicable law.

Where a request cannot be fulfilled, or can only be fulfilled in part, due to legal, regulatory, contractual, certification, record-retention, security, or other lawful requirements, LSR may retain or continue processing the relevant personal data to the extent permitted or required by applicable law.

Nothing in this section limits an individual's right to contact or lodge a complaint with a competent data protection or supervisory authority where such right is available under applicable law.

3. Personal Data We Collect

LSR may collect and process different categories of personal data depending on the individual's relationship with LSR, their role within the Portal, the services requested, and the activities carried out through or in connection with the Portal.

Not every category described below is collected from every individual. LSR seeks to collect and process only personal data that is relevant and reasonably necessary for the applicable purpose.

3.1 Identity Information

LSR may collect personal data used to identify or verify an individual, including name, surname, date of birth, nationality, signature, photograph, identification numbers, and other identifying information where necessary for the relevant service or activity.

Where required for identity verification, authorization, classification, certification, regulatory compliance, or other legitimate purposes, identity information may also be obtained from passports, seafarer identification documents, certificates of competency, official identification documents, or similar records.

The specific identity information required may vary according to the individual's role, the service requested, applicable regulatory requirements, and the level of verification necessary for the relevant activity.

3.2 Contact Information

LSR may collect contact information necessary in connection with the Portal, LSR services, and classification, certification, survey, audit, inspection, and other maritime activities.

Such information may include email addresses, telephone numbers, business addresses, mailing addresses, and other contact details provided to LSR or lawfully obtained from other sources.

Contact information may be used for account administration, authentication, operational correspondence, service-related communications, survey or audit coordination, technical requests, security notifications, certification communications, and other legitimate purposes associated with the relationship between LSR and the individual or organization.

Where required by applicable rules, regulations, statutory requirements, certification procedures, document formats, or the nature of the relevant service, contact information may also be included in certificates, reports, endorsements, statements, records, or other official or operational documents issued, maintained, or processed by LSR.

Individuals and organizations are responsible for providing accurate contact information and for updating such information where appropriate.

3.3 Account and Authentication Information

Where an individual is granted access to the Portal, LSR may process information necessary to create, administer, authenticate, secure, and maintain the individual's user account.

This may include usernames, account identifiers, assigned roles and permissions, company affiliation, account status, authentication records, password-related security information, verification records, session information, and records relating to account creation, modification, suspension, or termination.

Passwords shall be protected using appropriate security measures and should not be stored or made available in a form that permits ordinary retrieval of the user's original password.

LSR may also process authentication and access information for the purpose of detecting unauthorized access, investigating suspicious activity, maintaining audit trails, and protecting the security and integrity of the Portal.

3.4 Company and Professional Information

LSR may process information relating to an individual's professional role, employment, organizational affiliation, authority, and relationship with a company, vessel, or other organization.

Such information may include company name, position or job title, department, professional contact details, assigned responsibilities, authority to represent an organization, user role, professional qualifications, licenses, certificates, and other information relevant to the individual's professional capacity.

Where necessary, LSR may request or process documentation demonstrating an individual's authority to act on behalf of a company or organization or their qualifications to perform a particular professional activity.

Professional information may be used to determine access permissions, verify authority, administer services, assess eligibility, maintain records, and support classification, certification, survey, audit, and other LSR activities.

3.5 Vessel and Maritime Information

LSR may process information relating to vessels and maritime activities where such information contains or can reasonably be associated with an identifiable individual.

This may include information concerning vessel ownership, management, operation, authorized representatives, masters, officers, crew members, surveyors, auditors, technical personnel, and other persons associated with a vessel or maritime activity.

Vessel-related records may include names, professional roles, qualifications, signatures, contact information, responsibilities, declarations, survey or audit participation, certification records, and other information contained within vessel documentation.

Information relating solely to a vessel or legal entity and which does not identify or relate to a natural person is not personal data for the purposes of this Privacy Policy, except where applicable law provides otherwise.

3.6 Application, Survey and Certification Information

LSR may process personal data contained in or generated through applications, service requests, surveys, inspections, audits, technical reviews, classification activities, statutory certification processes, and other professional services provided by LSR.

Such information may include applicant details, authorized representatives, surveyor or auditor information, declarations, findings, comments, approvals, signatures, professional qualifications, correspondence, workflow actions, review records, and information contained within supporting documentation.

LSR may also maintain records identifying individuals who submit, review, approve, modify, reject, or otherwise participate in a particular application, survey, audit, certification, or related process.

These records may be maintained for operational traceability, certification integrity, quality assurance, legal and regulatory compliance, audit, security, and evidentiary purposes.

3.7 Documents and Uploaded Content

LSR may process personal data contained within documents, files, forms, certificates, reports, photographs, correspondence, declarations, drawings, supporting evidence, and other content uploaded, submitted, generated, or otherwise made available through the Portal.

The nature of personal data contained within such materials will depend upon the relevant document and the purpose for which it is submitted.

Users and organizations should submit only personal data that is relevant and reasonably necessary for the applicable service, request, legal obligation, regulatory requirement, or other legitimate purpose.

Where documents contain personal data relating to individuals other than the person submitting the document, the submitting party is responsible for ensuring that the information is provided to LSR lawfully and that any required notices, permissions, or other requirements have been satisfied.

3.8 Communications and Correspondence

LSR may process personal data contained in communications between individuals, organizations, and LSR.

This may include emails, Portal messages, support requests, technical correspondence, comments, notifications, clarification requests, responses, and other communications relating to LSR services or Portal activities.

Communications may be retained where necessary for operational continuity, service administration, quality assurance, security, dispute resolution, certification records, regulatory compliance, or other legitimate purposes.

3.9 Technical, Device and Usage Information

When individuals access or use the Portal, LSR may automatically collect or generate certain technical and usage information necessary for operation, security, administration, performance monitoring, and improvement of the Portal.

Such information may include Internet Protocol (IP) addresses, browser type and version, operating system, device type, session information, access times, referring pages, requested pages, navigation activity, language settings, screen or display information, and other technical information associated with Portal access.

Where permitted and appropriate, technical information may also be used to identify unusual activity, diagnose technical problems, understand Portal usage, improve performance, and protect LSR systems and users.

The collection and use of cookies and similar technologies are further described in Section 12 of this Privacy Policy.

3.10 Log, Security and Audit Information

LSR may generate and retain logs and audit records relating to activities performed through the Portal and associated systems.

Such records may include authentication events, login attempts, timestamps, IP addresses, user and account identifiers, session records, document uploads or downloads, workflow actions,

approvals, modifications, administrative actions, permission changes, security events, system errors, and other activities relevant to the operation and security of the Portal.

LSR may process such information for cybersecurity, access control, fraud prevention, incident investigation, operational traceability, quality assurance, compliance, dispute resolution, and evidentiary purposes.

Access to security and audit information may be restricted according to role, operational necessity, confidentiality requirements, and applicable law.

3.11 Information Received from Third Parties

LSR may receive personal data from third parties where such information is necessary or appropriate for the provision of services, verification of information, regulatory compliance, certification activities, security, or other lawful purposes.

Such sources may include shipowners, managers, operators, employers, authorized representatives, flag administrations, maritime authorities, port state authorities, recognized organizations, classification societies, surveyors, auditors, service providers, professional advisers, public registers, official databases, and other legitimate sources.

Personal data obtained from third parties may be combined with information already held by LSR where necessary for the relevant processing purpose and where permitted by applicable law.

Where required by applicable data protection law, LSR will provide individuals with information regarding the processing of personal data obtained from sources other than the individual, subject to any applicable exemptions or limitations.

4. How We Collect Personal Data

LSR may collect personal data through different sources and methods depending on the individual's relationship with LSR, the services involved, the relevant regulatory or operational requirements, and the manner in which the Portal is used.

Personal data may be collected directly from individuals, provided by organizations or authorized representatives, generated through the use of the Portal and associated systems, obtained from public or official sources, or received from third parties and service providers.

LSR seeks to collect personal data through lawful and appropriate means and to process such information in accordance with the purposes and legal bases described in this Privacy Policy.

4.1 Information Provided Directly by You

LSR may collect personal data that individuals provide directly when interacting with LSR or using the Portal.

This may include information provided during account registration, identity or authority verification, company or vessel registration, applications, service requests, surveys, audits, inspections, technical reviews, classification or certification processes, document submissions, communications, support requests, declarations, forms, and other interactions with LSR.

Individuals may also provide personal data when updating their account or professional information, responding to requests for clarification or additional documentation, participating in workflows, submitting comments or approvals, or communicating with LSR through the Portal, email, or other authorized communication channels.

Individuals should provide only information that is accurate, relevant, and reasonably necessary for the relevant purpose and should avoid submitting unnecessary personal data.

4.2 Information Provided by Your Organisation

Where an individual acts for or is associated with a company, shipowner, manager, operator, employer, vessel, or other organization, LSR may receive personal data relating to that individual from the relevant organization or its authorized representatives.

Such information may include identity and contact information, professional position, organizational affiliation, authority, assigned responsibilities, account permissions, qualifications, signatures, and information contained in documents, applications, declarations, or other records submitted by the organization.

Organizations may also provide personal data relating to directors, authorized signatories, company administrators, employees, vessel personnel, survey participants, representatives, consultants, contractors, or other individuals where such information is necessary for an LSR service or process.

Organizations and their authorized representatives are responsible for ensuring that personal data provided to LSR is submitted lawfully and that any information, notice, authorization, or other requirement applicable to such disclosure has been satisfied.

4.3 Information Generated Through Use of the Platform

LSR may automatically generate or collect personal data and technical information when individuals access, navigate, or perform activities through the Portal and associated systems.

This may include authentication events, login attempts, session information, timestamps, IP addresses, browser and device information, pages or functions accessed, workflow actions, document activities, approvals, changes, communications, administrative actions, system events, and security-related information.

Certain records may be generated automatically as part of the Portal's workflow, audit, security, document management, certification, or operational functions and may be associated with the user account or individual responsible for the relevant activity.

Such information may be used for Portal operation, security, access control, operational traceability, audit, troubleshooting, quality assurance, fraud prevention, compliance, service improvement, and other legitimate purposes described in this Privacy Policy.

4.4 Information Obtained from Public and Official Sources

LSR may obtain personal data from publicly available or official sources where such information is relevant and reasonably necessary for the provision of services, verification, classification, certification, compliance, security, or other lawful activities.

Such sources may include public registers, company registers, vessel registers, maritime databases, records maintained by flag administrations or competent authorities, regulatory publications, official sanctions or compliance sources, professional registers, and other publicly accessible or officially maintained information sources.

Information obtained from such sources may be used to verify information provided to LSR, establish or confirm professional or organizational relationships, assess eligibility or authority, support technical or regulatory processes, or comply with applicable legal and regulatory obligations.

The fact that information is publicly available does not, by itself, remove its status as personal data. LSR will process such information in accordance with applicable data protection requirements where it relates to an identifiable individual.

4.5 Information Received from Third Parties and Service Providers

LSR may receive personal data from third parties where necessary or appropriate for the provision, administration, verification, security, or compliance of LSR services and activities.

Such third parties may include shipowners, managers, operators, flag administrations, maritime and port authorities, recognized organizations, classification societies, surveyors, auditors, consultants, contractors, professional advisers, technology providers, hosting or communication providers, verification services, and other organizations involved in or supporting relevant LSR processes.

The categories of personal data received will depend on the relevant relationship and service and may include identity, contact, professional, organizational, verification, technical, certification, security, or other information necessary for the applicable purpose.

Where LSR receives personal data from a service provider acting on its behalf, the provider may process or transmit such information subject to applicable contractual, confidentiality, security, and data protection requirements.

Where required by applicable law, LSR will provide appropriate information regarding personal data obtained indirectly and the sources or categories of sources from which such data was obtained, subject to applicable legal exemptions or limitations.

5. Purposes of Processing Personal Data

LSR processes personal data only for specified, legitimate, and appropriate purposes connected with the operation of the Portal, the provision of LSR services, maritime classification and certification activities, legal and regulatory obligations, security, and other activities described in this Privacy Policy.

The purposes for which personal data is processed may vary depending on the individual's relationship with LSR, the services requested, the individual's professional role, applicable legal or regulatory requirements, and the nature of the relevant processing activity.

Personal data will not be used for purposes that are incompatible with the purposes for which it was originally collected unless such further processing is permitted or required by applicable law.

5.1 Account Creation and Administration

LSR may process personal data to create, activate, maintain, administer, modify, secure, suspend, or terminate user accounts within the Portal.

This processing may include verifying user information, establishing account credentials, associating users with relevant organizations, assigning roles and permissions, managing authentication, maintaining account status, administering access rights, and recording changes made to user accounts.

Personal data may also be processed to provide account-related assistance, resolve access problems, maintain accurate user records, and ensure that Portal access remains limited to appropriately authorized individuals.

Account and access records may be retained where necessary for security, audit, compliance, dispute resolution, or other legitimate purposes, including after an account has been suspended or terminated where permitted or required by applicable law.

5.2 Company and User Verification

LSR may process personal data to verify the identity of individuals, their association with an organization, their professional capacity, and their authority to access the Portal or act on behalf of a company, vessel, or other organization.

Verification may involve reviewing identification information, company records, professional information, authorization documents, signatures, licenses, certificates, declarations, or other supporting documentation relevant to the verification process.

LSR may also compare submitted information with information obtained from official records, competent authorities, public sources, or other legitimate sources where necessary and permitted by applicable law.

Verification activities are carried out to protect the integrity of LSR services, prevent unauthorized representation or access, establish appropriate permissions, support regulatory and compliance requirements, and ensure that actions performed through the Portal can be appropriately attributed to authorized individuals.

5.3 Vessel Registration and Management

LSR may process personal data where necessary to register, identify, administer, maintain, or manage vessels and their relationships with individuals and organizations within LSR systems.

This may include information concerning vessel owners, managers, operators, authorized representatives, masters, officers, crew members, technical personnel, surveyors, auditors, and

other individuals whose identity, role, authority, qualification, or involvement is relevant to the vessel or the services provided by LSR.

Personal data may be processed to establish and maintain vessel profiles, verify ownership or management relationships, record authorized representatives, administer vessel-related requests, maintain vessel histories, and associate relevant documents, certificates, surveys, audits, communications, and other records with the appropriate vessel and parties.

Where personal information is required to appear in vessel records, certificates, reports, endorsements, or other official documentation, LSR may process and reproduce such information to the extent necessary for the relevant document, service, regulatory requirement, or certification process.

5.4 Classification and Certification Services

LSR may process personal data where necessary to receive, assess, administer, perform, document, approve, issue, maintain, suspend, withdraw, renew, or otherwise manage classification and certification services.

This may include processing personal data contained in applications, technical submissions, survey and inspection records, audit records, declarations, supporting documents, approvals, certificates, endorsements, reports, correspondence, and other records relevant to classification or certification activities.

LSR may process information identifying applicants, authorized representatives, surveyors, auditors, reviewers, approvers, signatories, vessel personnel, and other individuals involved in the relevant process in order to establish responsibility, authority, professional capacity, and traceability.

Where required, personal data may be included in certificates, endorsements, reports, statements, verification records, or other official documents issued or maintained by LSR.

Personal data may also be retained as part of the historical record of classification and certification activities where necessary to demonstrate compliance, maintain certification integrity, support audits, respond to competent authorities, or satisfy legal, regulatory, contractual, or professional requirements.

5.5 Survey, Audit and Inspection Activities

SR may process personal data in connection with surveys, audits, inspections, examinations, verifications, assessments, and other attendance or review activities carried out by or on behalf of LSR.

Such processing may include information identifying surveyors, auditors, inspectors, vessel personnel, company representatives, responsible officers, witnesses, technical personnel, and other individuals participating in or relevant to the activity.

Personal data may be recorded in survey reports, audit records, inspection findings, checklists, attendance records, photographs, declarations, corrective action records, correspondence, supporting documentation, and other materials generated or received during the relevant activity.

LSR may process such information to plan and coordinate activities, verify authority and qualifications, document attendance and findings, assign responsibility, follow corrective actions, maintain traceability, demonstrate compliance, and support classification, certification, statutory, quality, safety, or other professional requirements.

5.6 Application and Request Management

LSR may process personal data to receive, identify, route, review, administer, track, respond to, approve, reject, place on hold, complete, or otherwise manage applications, requests, submissions, and related workflows.

This may include information identifying the person or organization making a request, individuals participating in the workflow, assigned personnel, reviewers, approvers, authorized representatives, and other persons associated with the relevant application or request.

LSR may maintain records of submissions, status changes, comments, clarifications, approvals, rejections, assignments, timestamps, communications, supporting documents, and other actions taken during the lifecycle of an application or request.

Such processing supports operational management, accountability, traceability, service delivery, quality assurance, security, compliance, and the maintenance of an accurate history of activities performed through the Portal.

5.7 Communications and Notifications

LSR may process personal data to communicate with users, organizations, representatives, vessel personnel, surveyors, auditors, authorities, service providers, and other relevant parties in connection with LSR services and activities.

Communications may include operational correspondence, requests for information or documentation, application updates, survey or audit coordination, certification notices, account communications, security alerts, technical notifications, service updates, support responses, regulatory communications, and other messages relevant to the relationship with LSR.

LSR may use contact information and Portal account information to determine the appropriate recipient and communication channel and to maintain records of communications where necessary.

Communications may be delivered through the Portal, email, telephone, or other communication channels appropriate to the relevant purpose and circumstances.

5.8 Document and Certificate Management

LSR may process personal data to create, receive, review, verify, approve, issue, distribute, store, retrieve, amend, renew, archive, suspend, withdraw, invalidate, or otherwise manage documents and certificates associated with LSR services.

Personal data may be contained in certificates, endorsements, reports, forms, declarations, applications, supporting documentation, technical records, verification records, correspondence, and other documents maintained within LSR systems.

Where necessary, LSR may use personal data to identify document owners, applicants, representatives, signatories, issuing or approving personnel, surveyors, auditors, responsible persons, and other individuals associated with a document or certificate.

LSR may also maintain document versions, issuance records, approval histories, verification information, timestamps, and other records necessary to establish authenticity, validity, status, accountability, and traceability.

5.9 Platform Security and Fraud Prevention

LSR may process personal data and technical information to protect the confidentiality, integrity, availability, authenticity, and security of the Portal, LSR systems, accounts, documents, certification processes, and associated services.

This may include monitoring authentication events, access activity, IP addresses, device and browser information, session activity, permission changes, administrative actions, unusual behavior, failed access attempts, and other security-related events.

LSR may use such information to detect, prevent, investigate, and respond to unauthorized access, account compromise, identity misuse, fraudulent submissions, document manipulation, misuse of certificates, malicious activity, security incidents, and other threats to LSR, its users, clients, systems, or services.

Where appropriate, LSR may take protective measures including additional verification, access restrictions, session termination, account suspension, investigation, preservation of relevant records, or notification to competent authorities where permitted or required by applicable law.

5.10 Legal and Regulatory Compliance

LSR may process personal data where necessary to comply with legal, regulatory, statutory, administrative, judicial, classification, certification, or other requirements applicable to LSR or the services it provides.

This may include compliance with requirements arising from applicable laws, maritime conventions, flag administrations, competent authorities, port state authorities, courts, regulatory bodies, recognized organization arrangements, certification requirements, sanctions or compliance obligations, and other legally applicable requirements.

Personal data may be used to respond to lawful requests, inspections, investigations, audits, reporting obligations, record-keeping requirements, verification activities, or other compliance processes.

Where required or permitted by applicable law, LSR may disclose relevant personal data to competent authorities or other authorized recipients in connection with such obligations.

5.11 Service Improvement and Analytics

LSR may process usage, technical, operational, and other relevant personal data to understand how the Portal and LSR services are used, assess performance, identify technical or operational

issues, improve functionality, enhance user experience, and support the development of services and systems.

This may include analyzing Portal usage patterns, page and feature interactions, system performance, errors, service activity, workflow efficiency, device or browser characteristics, and other information relevant to the performance and improvement of LSR systems and services.

Where reasonably practicable and appropriate for the relevant purpose, LSR may use aggregated, de-identified, or anonymized information to reduce the amount of identifiable personal data used for analytics and service improvement.

Information that has been irreversibly anonymized so that an individual can no longer be identified is not treated as personal data under this Privacy Policy to the extent that it no longer constitutes personal data under applicable law.

5.12 Establishment, Exercise and Defence of Legal Claims

LSR may process and retain personal data where reasonably necessary to establish, exercise, protect, or defend legal rights, claims, interests, or obligations.

This may include personal data contained in contracts, applications, communications, audit records, system logs, documents, certificates, survey or inspection records, approvals, declarations, transaction histories, security records, and other information relevant to an actual or potential legal claim, dispute, investigation, proceeding, or enforcement matter.

Personal data may be disclosed to courts, competent authorities, legal advisers, insurers, experts, auditors, or other authorized parties where such disclosure is necessary and permitted by applicable law.

Where personal data is required for an existing or reasonably anticipated legal claim, LSR may retain the relevant information beyond its ordinary retention period to the extent necessary and permitted by applicable law.

6. Legal Bases for Processing

LSR processes personal data only where there is an appropriate legal basis for the relevant processing activity.

The applicable legal basis will depend on the nature of the personal data, the purpose of the processing, the individual's relationship with LSR, the service involved, and the legal or regulatory framework applicable to the relevant activity.

Depending on the circumstances, LSR may rely on one or more of the legal bases described below. Where multiple legal bases may apply, LSR will determine the appropriate basis according to the specific processing activity and applicable law.

LSR does not rely on consent where another lawful basis is more appropriate for the relevant processing activity.

6.1 Performance of a Contract

LSR may process personal data where such processing is necessary to enter into, administer, perform, manage, or enforce a contract, service arrangement, or other legally binding relationship with an individual or an organization with which the individual is associated.

This may include processing necessary to provide requested services, administer Portal access, manage applications and service requests, carry out surveys, audits, inspections, technical reviews, classification or certification activities, issue or maintain documents, communicate regarding services, and perform other contractual or operational obligations.

Where an individual takes steps at their own request prior to entering into a contract, LSR may also process personal data where necessary to respond to those steps or assess the requested service.

Where the relevant contract is with an organization rather than the individual personally, another legal basis, such as legitimate interests or legal obligations, may apply to the processing of personal data relating to the organization's representatives, employees, or other associated individuals.

6.2 Compliance with Legal Obligations

LSR may process personal data where necessary to comply with a legal, statutory, regulatory, administrative, judicial, or other binding obligation applicable to LSR or the services it provides.

Such obligations may arise from applicable laws, maritime conventions, statutory certification requirements, flag administrations, competent authorities, courts, regulatory bodies, recognized organization arrangements, sanctions regimes, financial or accounting requirements, record-keeping obligations, or other legally binding requirements.

Processing may include collecting, verifying, retaining, reporting, disclosing, or otherwise using personal data where required to satisfy such obligations.

Where LSR is legally required to retain or disclose personal data, the relevant processing may continue notwithstanding a request for deletion or objection, to the extent required by applicable law.

6.3 Legitimate Interests

LSR may process personal data where such processing is necessary for legitimate interests pursued by LSR or, where permitted by applicable law, by a third party, provided that those interests are not overridden by the fundamental rights, freedoms, or interests of the individual.

Legitimate interests may include operating and administering the Portal, maintaining security, preventing fraud and misuse, verifying authority and identity, managing professional relationships, maintaining operational records, improving services, ensuring traceability, protecting certification integrity, supporting quality assurance, resolving disputes, defending legal claims, and maintaining the continuity and reliability of LSR operations.

Before relying on legitimate interests, LSR will consider the nature of the processing, the necessity of the processing, the reasonable expectations of the individuals concerned, and the potential impact on their rights and freedoms.

Where required by applicable law, individuals may have the right to object to processing based on legitimate interests.

6.4 Consent

LSR may process personal data on the basis of an individual's consent where consent is an appropriate and legally valid basis for the relevant processing activity.

Where LSR relies on consent, the consent will be sought in a manner intended to be specific, informed, freely given, and unambiguous, as required by applicable law.

Consent may be requested separately from acceptance of the Terms of Use or acknowledgement of this Privacy Policy and may relate to a specific processing activity, feature, communication, or other defined purpose.

Where processing is based on consent, the individual may withdraw that consent at any time, subject to applicable law. Withdrawal of consent will not affect the lawfulness of processing carried out before the withdrawal.

Withdrawal of consent will also not affect processing that is necessary or permitted on another lawful basis.

6.5 Protection of Vital Interests

LSR may process personal data where such processing is necessary to protect the vital interests of an individual or another natural person, where this legal basis is available under applicable law.

This basis may apply in exceptional circumstances involving serious and immediate risks to life, health, safety, or physical integrity, particularly where the individual concerned is unable to provide consent or where obtaining consent is not reasonably practicable.

Given the maritime nature of LSR activities, such circumstances may include emergency situations involving vessels, personnel, accidents, casualties, safety incidents, or other urgent situations where processing personal data is necessary to protect individuals.

LSR will rely on this legal basis only where the circumstances and applicable law justify its use.

6.6 Other Applicable Legal Bases

Depending on the jurisdiction, nature of the processing activity, category of personal data, or specific legal framework applicable to a particular LSR service, additional or alternative legal bases may apply.

Such bases may include processing necessary for the performance of a task carried out in the public interest, exercise of official authority, compliance with maritime or statutory functions, establishment or defence of legal claims, or other grounds expressly recognized under applicable law.

Where a specific legal or regulatory framework imposes additional requirements or provides a particular lawful basis for processing, LSR may rely on that basis to the extent applicable.

This Privacy Policy does not limit LSR to a particular legal basis where applicable law provides another lawful and appropriate ground for processing.

7. Special Categories and Sensitive Information

LSR may, in limited circumstances, process personal data that is considered sensitive, specially protected, or subject to additional legal requirements under applicable data protection laws.

The nature and extent of such processing will depend on the relevant service, legal or regulatory requirements, the individual's role, the documents involved, and the specific circumstances of the processing activity.

LSR does not seek to collect sensitive or specially protected personal data unless such information is relevant and reasonably necessary for a legitimate purpose, or where its processing is required or permitted by applicable law.

Where additional safeguards, conditions, or legal requirements apply to the processing of sensitive or specially protected personal data, LSR will process such information in accordance with those requirements.

7.1 Special Categories of Personal Data

Depending on applicable law, certain types of personal data may be subject to enhanced protection or may be classified as special categories of personal data.

Such information may include, where relevant and legally recognized as specially protected, information concerning health, biometric characteristics used for identification, racial or ethnic origin, religious or philosophical beliefs, political opinions, trade union membership, genetic information, sexual life or sexual orientation, or other categories afforded enhanced protection under applicable law.

LSR does not ordinarily require such information for general Portal access or routine account administration.

However, limited processing may occur where such information is contained in documents or records submitted in connection with a specific service, regulatory requirement, safety matter, legal obligation, professional qualification, medical or fitness documentation, identity verification process, or other legitimate activity.

Where LSR processes special categories of personal data, such processing will be carried out only where an appropriate legal basis and any additional condition required under applicable law are satisfied.

7.2 Identification and Official Documents

LSR may process official identification documents and other documents containing sensitive or high-risk personal information where such documentation is necessary for identity verification, authority verification, professional qualification, regulatory compliance, certification, security, or other legitimate purposes.

Such documents may include passports, seafarer identity documents, national identification documents, certificates of competency, professional licenses, authorization documents, signature records, company authorization records, or other official documents relevant to the individual's role or the service provided by LSR.

Official identification documents may contain information beyond what is necessary for a particular purpose. LSR seeks to limit access to and use of such documents to authorized personnel and to the extent reasonably necessary for the relevant activity.

Where practicable and appropriate, LSR may record or retain only the information required from an official document rather than retaining the entire document, subject to applicable legal, regulatory, certification, security, and record-keeping requirements.

Copies of official identification documents will not be treated as publicly available information merely because the underlying identity details may appear in other records or sources.

7.3 Processing Restrictions and Safeguards

LSR applies additional restrictions and safeguards where personal data is sensitive, specially protected, high-risk, or otherwise requires enhanced protection.

Such safeguards may include restricted access, role-based permissions, authentication controls, secure transmission, encryption where appropriate, logging and monitoring of access, confidentiality obligations, data minimization, retention controls, and other technical or organizational measures appropriate to the nature and risk of the processing.

Access to sensitive or specially protected personal data will be limited, where practicable, to individuals whose duties reasonably require access to such information.

LSR may also restrict the downloading, copying, export, modification, disclosure, or further use of sensitive records where necessary to protect the individual, preserve the integrity of records, comply with applicable law, or maintain security and confidentiality.

Sensitive or specially protected personal data will not be used for unrelated purposes solely because LSR possesses or has access to such information.

Where personal data is no longer required for the applicable purpose, LSR may delete, anonymize, archive, restrict, or otherwise manage the information in accordance with applicable legal, regulatory, certification, contractual, security, and retention requirements.

8. Sharing and Disclosure of Personal Data

LSR may share or disclose personal data where such disclosure is necessary or appropriate for the provision of services, classification and certification activities, regulatory compliance, security, legal obligations, professional cooperation, or other legitimate purposes described in this Privacy Policy.

Personal data will not be disclosed to third parties without an appropriate purpose and legal basis. The scope of any disclosure will depend on the nature of the relevant service, the role of the recipient, applicable legal or regulatory requirements, contractual arrangements, and the circumstances of the processing activity.

Where reasonably practicable, LSR will limit disclosures to the personal data necessary for the relevant purpose and may apply contractual, technical, organizational, confidentiality, or other safeguards appropriate to the nature of the information and the recipient.

8.1 Flag Administrations and Maritime Authorities

LSR may disclose personal data to flag administrations, maritime administrations, and other authorities having responsibility for vessels, statutory certification, maritime safety, security, environmental protection, seafarer matters, or other maritime functions.

Such disclosure may occur where required or appropriate in connection with statutory certification, authorization, survey and audit activities, vessel status, regulatory reporting, verification, investigations, compliance matters, or other official maritime processes.

The information disclosed may include identity, contact, professional, authorization, survey, audit, certification, vessel-related, document, or other information relevant to the authority's lawful function.

Where LSR acts under authorization, delegation, recognition, agreement, or another formal arrangement with a flag administration or maritime authority, personal data may be exchanged to the extent necessary to perform, administer, verify, or demonstrate compliance with the relevant functions.

8.2 Port State and Other Competent Authorities

LSR may disclose personal data to port state authorities, governmental bodies, regulatory authorities, law enforcement bodies, courts, administrative authorities, or other competent authorities where such disclosure is required or permitted by applicable law or is necessary in connection with a lawful official function.

Such disclosures may relate to inspections, investigations, enforcement actions, vessel detention or deficiency matters, verification of certificates, safety or security incidents, legal proceedings, regulatory reporting, compliance reviews, or other matters within the authority's competence.

LSR may verify the nature and scope of a request before disclosing personal data and may limit the disclosure to information reasonably necessary to respond to the relevant lawful request or obligation.

Where applicable law permits or requires, LSR may notify the affected individual or organization regarding such disclosure, unless notification is prohibited, restricted, or would adversely affect the relevant investigation, proceeding, security measure, or legal obligation.

8.3 Recognized Organisations and Classification Societies

LSR may share personal data with recognized organizations, classification societies, technical organizations, or similar professional bodies where such sharing is necessary or appropriate for classification, statutory certification, transfer of class, verification, technical cooperation, regulatory compliance, or other legitimate maritime purposes.

Information shared may include vessel-related records, survey or audit information, certification records, professional identities, correspondence, technical submissions, approvals, or other information relevant to the applicable process.

Where a vessel transfers class, certification responsibility, management arrangements, or another relevant professional relationship, personal data contained within historical or current records may be transferred or made available where necessary for the continuity, verification, integrity, or regulatory requirements of the relevant process.

Any sharing will be subject to applicable law, professional requirements, relevant agreements, and appropriate confidentiality or data protection obligations.

8.4 Surveyors, Auditors and Authorized Personnel

LSR may make personal data available to surveyors, auditors, inspectors, reviewers, technical personnel, administrators, and other authorized individuals where access is necessary for them to perform duties or services on behalf of or in connection with LSR.

Such access may include information necessary to plan or perform surveys, audits, inspections, technical reviews, certification activities, document reviews, verification, corrective action follow-up, or other assigned professional responsibilities.

Access will be limited according to role, authorization, assigned responsibility, operational necessity, and applicable confidentiality and data protection requirements.

Surveyors, auditors, contractors, or other external authorized personnel may be subject to contractual, professional, confidentiality, security, or data protection obligations governing their access to and use of personal data.

8.5 Vessel Owners, Managers and Other Authorized Organisations

LSR may share personal data with vessel owners, managers, operators, DOC holders, agents, employers, charterers, consultants, representatives, or other organizations where such sharing is necessary for the provision, coordination, administration, verification, or completion of an LSR service or maritime process.

The information shared will depend on the relevant relationship, authorization, service, and role of the recipient and may include application information, survey or audit records, certification

information, requests, communications, documents, status information, or information identifying individuals involved in the relevant process.

LSR may apply access controls, organizational relationships, user roles, permissions, or other mechanisms to determine which information an organization or its authorized users may access through the Portal.

Access to personal data through an organizational relationship does not authorize the recipient to use that information for unrelated purposes or to disclose it further without an appropriate legal basis.

8.6 Service Providers and Technology Partners

LSR may engage third-party service providers and technology partners to support the operation, hosting, maintenance, security, communication, storage, backup, authentication, software, infrastructure, analytics, technical support, or other functions necessary for LSR systems and services.

Such providers may process personal data only to the extent necessary to perform the relevant services or functions and subject to applicable contractual and legal requirements.

Where a provider processes personal data on behalf of LSR, LSR may require appropriate provisions concerning confidentiality, security, permitted processing, data retention, incident management, sub-processing, international transfers, deletion or return of data, and other data protection obligations appropriate to the service.

The use of a service provider does not, by itself, permit the provider to use personal data for its own unrelated purposes.

8.7 Professional and Legal Advisers

LSR may disclose personal data to legal advisers, accountants, auditors, insurers, consultants, experts, compliance professionals, or other professional advisers where access to such information is reasonably necessary for the provision of professional services to LSR.

Such disclosure may occur in connection with legal advice, claims, disputes, audits, financial matters, regulatory compliance, insurance matters, risk management, investigations, contractual matters, governance, or other professional functions.

Professional advisers receiving personal data may be subject to professional duties, confidentiality obligations, contractual requirements, legal restrictions, or other protections governing the use and disclosure of such information.

8.8 Disclosure Required by Law

LSR may disclose personal data where required by applicable law, regulation, court order, legal process, governmental request, regulatory requirement, or other binding legal obligation.

LSR may also disclose personal data where permitted by applicable law and reasonably necessary to investigate or prevent unlawful activity, protect the rights, safety, security, or property of LSR or others, respond to emergencies, enforce legal rights, or cooperate with competent authorities.

Where appropriate, LSR may assess the validity, authority, scope, and proportionality of a request before making a disclosure.

LSR may retain records of legally required disclosures where necessary for accountability, compliance, security, audit, or evidentiary purposes.

8.9 Corporate Transactions and Organisational Changes

If LSR undergoes or considers a merger, acquisition, restructuring, reorganization, transfer of business, transfer of assets, change of ownership, joint venture, insolvency process, succession, or another significant organizational or corporate transaction, personal data may be disclosed or transferred where reasonably necessary in connection with that transaction.

Such information may be made available to prospective or actual counterparties, advisers, auditors, financiers, insurers, authorities, or other parties involved in the transaction, subject to appropriate confidentiality and data protection safeguards where applicable.

Any recipient acquiring or assuming relevant LSR operations, services, systems, rights, or obligations may continue processing personal data for purposes consistent with those for which the information was originally processed, subject to applicable law and any required notices.

Where applicable law requires notification, consent, or another safeguard in connection with a transfer of personal data resulting from a corporate or organizational change, LSR will take the required measures.

9. International Transfers of Personal Data

Due to the international nature of maritime activities and the services provided by LSR, personal data may be processed, accessed, disclosed, or transferred across national borders.

International transfers may arise in connection with classification and certification activities, surveys, audits, inspections, vessel operations, regulatory requirements, cooperation with flag administrations and maritime authorities, the use of service providers, or other activities described in this Privacy Policy.

Where personal data is transferred internationally, LSR will take into account applicable data protection laws and any requirements governing the transfer of personal data to another country or jurisdiction.

The level of data protection available in the destination country may differ from that applicable in the country from which the personal data originates. Where required by applicable law, LSR will implement appropriate safeguards or rely upon another legally recognized mechanism for the relevant transfer.

9.1 International Nature of LSR Services

LSR operates in an international maritime environment in which vessels, shipowners, managers, operators, surveyors, auditors, service providers, flag administrations, maritime authorities, and other relevant parties may be located in different countries or jurisdictions.

As a result, the provision and administration of LSR services may require personal data to be accessed, processed, communicated, or transferred between parties located in different countries.

For example, a vessel may operate under the flag of one State, be owned or managed by organizations established in other jurisdictions, undergo surveys or audits in another country, and receive services from LSR personnel or authorized professionals located elsewhere.

Personal data may therefore be transferred internationally where reasonably necessary for the performance, coordination, verification, documentation, certification, regulatory oversight, or administration of the relevant maritime activity or LSR service.

International processing or transfer does not remove the protections applicable to personal data, and LSR will apply relevant data protection requirements according to the circumstances and applicable law.

9.2 Transfers Outside the Country of Collection

Personal data collected in one country or jurisdiction may be transferred to, stored in, accessed from, or otherwise processed in another country where necessary for the purposes described in this Privacy Policy.

Such transfers may involve LSR operations, authorized personnel, surveyors, auditors, flag administrations, maritime authorities, classification societies, recognized organizations, service providers, professional advisers, or other authorized recipients located outside the country in which the personal data was originally collected.

The laws and data protection standards applicable in the destination country may differ from those applicable in the country of collection and may provide different rights, obligations, or levels of protection.

Where applicable law restricts international transfers, LSR will assess the relevant transfer and use an appropriate legal basis, safeguard, exception, authorization, or other transfer mechanism as required.

LSR will not treat the international nature of its activities as, by itself, removing or overriding restrictions imposed by applicable data protection law.

9.3 Transfer Safeguards

Where required by applicable law, LSR will implement appropriate safeguards for international transfers of personal data.

Depending on the applicable legal framework and circumstances of the transfer, such safeguards may include contractual protections, standard contractual clauses or equivalent mechanisms, binding arrangements, adequacy decisions or recognized jurisdictions, transfer agreements, confidentiality obligations, security requirements, access restrictions, encryption, or other legally recognized measures.

LSR may assess relevant factors concerning a transfer, including the nature and sensitivity of the personal data, the purpose and necessity of the transfer, the recipient, the destination country, applicable legal protections, and the technical and organizational measures available to protect the information.

Where LSR engages service providers that process personal data internationally, LSR may require appropriate contractual and security obligations concerning the processing, confidentiality, transfer, retention, access, return, or deletion of personal data.

Where applicable law permits an international transfer on the basis of a specific exception or derogation, LSR may rely upon that mechanism where the relevant legal conditions are satisfied.

9.4 Transfers to Maritime Authorities and Organisations

Due to the regulatory and international nature of maritime classification and statutory certification, LSR may be required or permitted to transfer personal data to flag administrations, maritime administrations, port state authorities, recognized organizations, classification societies, or other competent maritime bodies located in other countries or jurisdictions.

Such transfers may be necessary in connection with statutory certification, vessel surveys, audits, inspections, transfer of class, verification of certificates or records, regulatory reporting, investigations, casualty or safety matters, compliance activities, or the performance of functions authorized or required by a competent maritime authority.

Where an international transfer is necessary to perform a legal, regulatory, statutory, certification, or other official maritime function, LSR will determine the appropriate basis for the transfer in accordance with applicable law and the circumstances of the relevant activity.

The information transferred will, where reasonably practicable, be limited to information relevant and necessary for the applicable official or professional purpose.

Nothing in this section requires LSR to transfer personal data where such transfer would be unlawful under applicable data protection law.

10. Data Retention

LSR retains personal data only for as long as reasonably necessary for the purposes for which it was collected or processed, and for any additional period required or permitted by applicable legal, regulatory, contractual, certification, security, audit, operational, or professional obligations.

Retention periods may vary depending on the category of personal data, the nature of the relevant service, the individual's relationship with LSR, the type of record involved, applicable statutory or regulatory requirements, the need to maintain certification or audit history, and the potential need to establish, exercise, or defend legal claims.

LSR may retain certain records for longer periods where such retention is necessary to preserve the integrity and traceability of classification, certification, survey, audit, technical, security, or regulatory activities.

When personal data is no longer required for the applicable purposes and no further lawful basis exists for its retention, LSR may delete, anonymize, archive, restrict, or otherwise securely manage the information in accordance with applicable requirements and internal retention procedures.

10.1 General Retention Principles

LSR determines retention periods by considering the purpose for which personal data is processed, the nature and sensitivity of the information, operational requirements, legal and regulatory obligations, certification and audit requirements, security considerations, contractual commitments, and the potential need to preserve evidence or historical records.

Personal data will not be retained indefinitely solely because it may be technically possible to do so.

Where different retention requirements apply to the same information, LSR may retain the information for the longest period that is lawfully required or reasonably justified by the applicable purpose.

Retention periods may also be extended where records are subject to an ongoing investigation, dispute, audit, regulatory review, legal proceeding, security incident, or other matter that reasonably requires preservation of the information.

10.2 Account and User Records

LSR may retain user account records and associated personal data for as long as the account remains active and for an appropriate period following suspension, closure, termination, or expiry of access.

Such records may include identity and contact information, organizational affiliation, roles and permissions, verification records, account status, authentication records, access histories, administrative changes, and other information associated with the management and security of the account.

Certain account-related records may be retained after access ends where necessary for audit, security, compliance, investigation, dispute resolution, legal claims, prevention of unauthorized re-registration, or other legitimate purposes.

Where account information is no longer required, LSR may delete, anonymize, archive, or restrict the relevant records in accordance with applicable retention requirements.

10.3 Vessel, Survey and Certification Records

LSR may retain personal data contained within vessel, survey, audit, inspection, classification, certification, technical, and related records for periods appropriate to the relevant maritime activity and applicable professional, regulatory, contractual, or legal requirements.

Such records may include information identifying vessel owners, managers, operators, authorized representatives, masters, officers, crew members, surveyors, auditors, reviewers, approvers, signatories, technical personnel, or other individuals involved in the relevant process.

Retention of these records may be necessary to preserve vessel history, certification continuity, survey and audit traceability, technical decision records, regulatory compliance, certificate verification, transfer of class, investigations, or other professional requirements.

Where records form part of the historical classification or certification record of a vessel, LSR may retain such records beyond the duration of the immediate service relationship where reasonably necessary and permitted by applicable law.

10.4 Communications and Operational Records

LSR may retain communications and operational records where necessary to administer services, maintain an accurate history of interactions, support continuity of operations, demonstrate decisions or instructions, resolve disputes, maintain quality records, or comply with legal and regulatory requirements.

Such records may include emails, Portal messages, support requests, notifications, comments, clarification requests, workflow communications, correspondence with authorities, and other operational communications.

The retention period may depend on the subject matter, the associated service or vessel, the regulatory significance of the communication, and whether the record forms part of an application, certification, survey, audit, contractual, or legal file.

Routine communications that no longer have operational, legal, regulatory, security, or historical value may be deleted in accordance with applicable retention procedures.

10.5 Security and Audit Logs

LSR may retain security logs, audit trails, access records, authentication records, system events, administrative activity, and other technical records for periods necessary to maintain security, detect and investigate incidents, establish accountability, preserve operational traceability, and demonstrate compliance.

Such records may include timestamps, user identifiers, IP addresses, device and browser information, session records, login attempts, permission changes, document activity, workflow actions, system errors, alerts, and other security or operational metadata.

Retention periods for security and audit information may differ from those applicable to ordinary account or usage data due to the need to investigate incidents, identify patterns of misuse, preserve evidence, support audits, or respond to legal and regulatory requests.

Access to retained security and audit records may be limited to authorized personnel according to operational necessity and applicable security and confidentiality requirements.

10.6 Legal and Regulatory Retention Requirements

LSR may retain personal data for periods required by applicable laws, regulations, maritime conventions, statutory certification requirements, flag administrations, competent authorities, contractual obligations, recognized organization arrangements, accounting requirements,

insurance requirements, quality systems, or other binding or professional record-keeping requirements.

Where a mandatory retention period applies, LSR may retain the relevant personal data for that period even if the original operational purpose has ended or an individual requests deletion.

Where several mandatory or professional retention requirements apply, LSR may retain the relevant records for the period necessary to satisfy the applicable requirements.

LSR may also preserve records beyond ordinary retention periods where required by a legal hold, court order, regulatory instruction, investigation, pending claim, audit, or other binding requirement.

10.7 Deletion, Anonymisation and Archiving

When personal data is no longer required for the purpose for which it was processed and no further legal, regulatory, contractual, certification, security, audit, or other lawful basis requires its retention, LSR may securely delete, anonymize, archive, restrict, or otherwise dispose of the information.

Deletion methods may vary depending on the system, storage medium, backup architecture, nature of the data, and applicable security or technical requirements.

Where immediate deletion from backup systems is not technically practicable, personal data may remain in protected backups until it is overwritten or deleted according to the applicable backup cycle, provided that it is not restored or used for ordinary processing except where necessary for recovery, security, legal, or other lawful purposes.

Where information is anonymized, LSR will seek to ensure that the anonymization is sufficiently effective so that the individual is no longer identifiable by means reasonably likely to be used, having regard to applicable law and the circumstances of the processing.

Archived records may remain subject to access restrictions and other appropriate security measures and may be accessed only where necessary for the purpose for which the archive is maintained.

11. Data Security

LSR implements technical and organizational measures designed to protect personal data against unauthorized or unlawful access, use, disclosure, alteration, destruction, loss, or other forms of inappropriate processing.

The nature and level of security measures applied may vary depending on the sensitivity of the personal data, the nature of the processing activity, the systems involved, applicable legal or regulatory requirements, operational needs, and the risks associated with the processing.

LSR seeks to apply security measures that are proportionate to the nature and risk of the relevant processing and to review and improve such measures where appropriate.

No information system, electronic communication method, or storage environment can be guaranteed to be completely secure. Accordingly, while LSR takes reasonable steps to protect personal data, absolute security cannot be guaranteed.

11.1 Technical and Organisational Measures

LSR may implement technical and organizational measures appropriate to the systems, services, information, and risks involved in the processing of personal data.

Such measures may include access controls, authentication mechanisms, role-based permissions, encryption where appropriate, network and system security, secure communications, logging, monitoring, backup and recovery procedures, vulnerability management, software updates, secure configuration, data minimization, segregation of duties, confidentiality requirements, personnel controls, and incident response procedures.

LSR may periodically review security measures and modify them in response to changes in technology, operational requirements, identified risks, legal or regulatory requirements, or the development of LSR systems and services.

Security measures may differ between systems or processing activities depending on the nature and sensitivity of the relevant information and the risks associated with its processing.

11.2 Access Controls and Authorization

LSR may restrict access to personal data according to user roles, assigned responsibilities, organizational relationships, operational necessity, and the principle that access should be limited to individuals who require the information for legitimate purposes.

Access permissions may be established and managed through account roles, authorization levels, organizational relationships, workflow assignments, administrative controls, or other access-management mechanisms.

LSR may review, modify, suspend, or revoke access rights where necessary due to changes in responsibilities, organizational relationships, employment or contractual status, security concerns, or other relevant circumstances.

Users and organizations are responsible for ensuring that access granted under their authority remains appropriate and for promptly notifying LSR or taking appropriate action where an individual's authority changes or ends.

LSR may record access and administrative actions in audit logs to support accountability, security, compliance, and investigation of unauthorized activity.

11.3 Authentication and Account Security

LSR may use authentication and account-security mechanisms to verify the identity of users and protect Portal accounts from unauthorized access.

Such mechanisms may include usernames, passwords, verification codes, session controls, account status controls, device or network information, identity verification, multi-factor

authentication where implemented, or other authentication measures considered appropriate by LSR.

Users are responsible for maintaining the confidentiality of their credentials and authentication information and must not knowingly permit unauthorized persons to access their accounts.

LSR may require password changes, terminate active sessions, request additional verification, temporarily restrict access, suspend accounts, or apply other protective measures where account compromise or suspicious activity is suspected.

Authentication and security events may be logged and retained for security, audit, compliance, investigation, and evidentiary purposes.

11.4 Document and Data Protection

LSR may apply controls intended to protect documents, records, certificates, technical submissions, communications, and other information containing personal data throughout their lifecycle within LSR systems.

Such controls may include restrictions on viewing, downloading, copying, modifying, approving, exporting, sharing, or deleting information according to user roles, document status, operational requirements, and security needs.

LSR may maintain document versions, approval records, verification information, timestamps, digital references, audit histories, and other controls designed to preserve document integrity, authenticity, accountability, and traceability.

Where personal data is transferred or communicated electronically, LSR may use secure transmission methods, encryption, protected access mechanisms, or other appropriate technical safeguards depending on the nature and sensitivity of the information.

Access to archived or historical documents may remain restricted even where those documents are no longer part of an active workflow or service.

11.5 Monitoring and Audit Trails

LSR may monitor the operation and use of the Portal and associated systems for security, compliance, operational integrity, quality assurance, fraud prevention, troubleshooting, and other legitimate purposes.

Monitoring may include authentication events, access activity, system events, workflow actions, document activity, permission changes, administrative actions, unusual behavior, technical errors, and other activities relevant to system operation or security.

LSR may maintain audit trails recording who performed a particular action, the nature of the action, when it occurred, and other relevant technical or operational information.

Audit trails may be used to investigate incidents, verify transactions or approvals, establish accountability, resolve disputes, identify unauthorized activity, demonstrate compliance, and protect the integrity of classification, certification, document, and workflow processes.

Monitoring and audit activities will be carried out in accordance with applicable law and will not authorize the use of personal data for purposes unrelated to legitimate security, operational, compliance, or other lawful requirements.

11.6 Personal Data Breach Management

LSR may maintain procedures for identifying, assessing, containing, investigating, documenting, responding to, and recovering from actual or suspected personal data breaches or security incidents involving personal data.

Where an incident occurs, LSR may take measures including restricting access, terminating sessions, changing credentials, isolating affected systems, preserving logs and evidence, restoring systems or data, investigating the cause and scope of the incident, and implementing corrective or preventive measures.

LSR will assess personal data breaches in accordance with applicable data protection requirements, including the nature of the information affected, the circumstances of the incident, the potential consequences for individuals, and the measures available to mitigate relevant risks.

Where required by applicable law, LSR will notify the competent supervisory or data protection authority of a personal data breach within the applicable legal timeframe.

Where applicable law requires notification to affected individuals, LSR will provide such notification in accordance with the relevant legal requirements and may include information regarding the nature of the incident, potential effects, measures taken, and actions that affected individuals may reasonably take to protect themselves.

LSR may maintain records of security incidents and personal data breaches where necessary for legal compliance, accountability, security improvement, audit, investigation, or other legitimate purposes.

12. Cookies, Analytics and Similar Technologies

LSR may use cookies, local storage, session storage, and other similar storage or access technologies in connection with the operation, security, functionality, administration, and improvement of the Portal.

These technologies may store or access information on a user's device or browser and may be used to maintain sessions, authenticate users, preserve preferences, retain form progress, support workflow functionality, protect the Portal, analyze performance, and provide other features necessary or useful for the operation of LSR services.

The type, purpose, duration, and legal requirements applicable to a particular technology may vary depending on its function and the jurisdiction applicable to the user or processing activity.

Where applicable law requires consent before a particular cookie or similar technology may be used, LSR will seek the required consent before using that technology. Technologies that are strictly necessary to provide a service requested by the user or to perform essential Portal functionality may be used without consent where permitted by applicable law.

12.1 Cookies and Local Storage

The Portal may use cookies and browser-based storage technologies, including local storage and session storage, to store or retrieve information necessary for particular Portal functions.

Cookies may be used to maintain authentication or session state, apply security controls, remember certain settings or preferences, support navigation, and provide other functionality associated with the use of the Portal.

Local storage or similar browser storage may be used to preserve information on the user's device between pages, sessions, or visits where necessary to provide specific Portal functionality.

In particular, the Portal may use local storage to preserve form progress, temporary draft information, workflow state, navigation context, or other information necessary to enable features such as Save & Exit, returning to an incomplete form, restoring previously entered information, or continuing a process that has not yet been submitted.

The information stored through these technologies will depend on the relevant feature. LSR will seek to avoid storing sensitive personal data in browser storage where such storage is not necessary for the relevant functionality.

Information stored locally on a user's device may remain there until it expires, is removed by the Portal, is replaced by newer information, or is deleted through the user's browser or device settings, depending on the technology and implementation involved.

Deleting or disabling cookies, local storage, or other browser storage may result in the loss of saved form progress, preferences, authentication state, or other Portal functionality.

12.2 Essential Technologies

LSR may use cookies, local storage, session storage, and other technologies that are necessary for the operation, security, or functionality of the Portal or for the provision of services expressly requested by the user.

Essential technologies may be used for purposes including authentication, session management, security controls, access permissions, fraud prevention, load or system management, preservation of workflow state, temporary storage of information necessary to complete a process, and maintenance of user-requested functionality.

This category may also include browser storage necessary to preserve an incomplete form or draft so that a user can use a Save & Exit function and subsequently return to the relevant process without losing information that was intentionally saved.

Where a user requests functionality that requires information to be stored on or accessed from their device, the relevant storage technology may be considered necessary to provide that requested functionality where permitted by applicable law.

Because these technologies may be essential for particular Portal functions, disabling or deleting them may prevent authentication, cause saved information to be lost, interrupt workflows, prevent

restoration of unfinished forms, or make certain parts of the Portal unavailable or unable to operate as intended.

LSR will seek to use essential technologies only for purposes reasonably necessary to provide the relevant functionality, security, or service.

12.3 Analytics and Performance Technologies

LSR may use cookies or similar technologies to understand how the Portal is used, evaluate performance, identify technical problems, measure service activity, and improve functionality and user experience.

Depending on the technologies implemented, analytics information may include page visits, navigation paths, feature usage, session activity, referring information, device type, browser characteristics, operating system, screen information, performance metrics, errors, response times, and other information relating to use of the Portal.

Analytics may be conducted using LSR's own systems or, where appropriate, through authorized service providers subject to applicable contractual and data protection requirements.

Where reasonably practicable, LSR may aggregate, de-identify, or anonymize analytics information where identifiable personal data is not necessary for the relevant analytical purpose.

Where applicable law requires consent for analytics or performance technologies, such technologies will be activated only after the required consent has been obtained.

12.4 Security and Fraud-Prevention Technologies

LSR may use cookies, browser storage, device information, session identifiers, and other storage or access technologies to protect the Portal, user accounts, documents, services, and systems against unauthorized access, misuse, fraud, malicious activity, or other security threats.

These technologies may support authentication, session integrity, detection of suspicious activity, prevention of repeated unauthorized access attempts, security monitoring, account protection, request validation, and other security functions.

Security technologies may process technical information including IP addresses, session identifiers, device or browser characteristics, authentication events, access patterns, and other information necessary to identify or respond to security risks.

Where a security technology is necessary to provide secure access to the Portal or protect a service requested by the user, it may be used without consent where permitted by applicable law.

The use of security technologies will not, by itself, authorize the use of collected information for unrelated advertising, profiling, or other purposes that are not necessary for the relevant security function.

12.5 Cookie Preferences and Controls

Where LSR uses cookies or similar technologies that require user consent under applicable law, users may be provided with mechanisms to accept, reject, or manage those technologies.

Users may also be able to control or delete cookies, local storage, and other stored information through the settings provided by their browser or device.

Changing browser settings, deleting stored information, blocking storage technologies, or withdrawing consent may affect the availability or operation of certain Portal features.

In particular, deletion or blocking of local storage used for form progress, draft preservation, or workflow continuity may result in previously saved information being unavailable and may prevent features such as Save & Exit or return-to-form functionality from operating as intended.

Withdrawal of consent for a non-essential technology will not affect the lawfulness of processing performed before consent was withdrawn and will not prevent LSR from using technologies that remain necessary and lawful without consent under applicable law.

LSR may update the technologies used by the Portal as systems and functionality develop. Where required, users will be provided with updated information or choices regarding material changes to technologies that require consent.

13. Automated Processing and Artificial Intelligence

LSR may use automated systems, algorithms, artificial intelligence technologies, or other computer-assisted tools to support the operation, security, administration, analysis, and development of the Portal and LSR services.

Such technologies may be used to assist with workflow management, information processing, document handling, validation, security monitoring, risk identification, data analysis, search, classification of information, technical assistance, or other operational functions.

The use of automated or artificial intelligence-assisted technologies does not necessarily mean that decisions affecting an individual are made solely by automated means. Where appropriate, automated outputs may be used as supporting information for review, assessment, or decision-making by authorized personnel.

LSR will seek to use automated and artificial intelligence-assisted processing in a manner consistent with applicable data protection requirements, including requirements relating to lawfulness, transparency, data minimization, security, accuracy, and the protection of individuals' rights.

Where a processing activity involves automated decision-making subject to specific legal requirements, LSR will apply the safeguards required by applicable law.

13.1 Automated Processing

LSR may use automated processing to perform or support routine, technical, administrative, analytical, security, and operational activities within the Portal and associated systems.

Automated processing may include routing applications or requests, assigning workflow stages, validating required fields, identifying incomplete submissions, generating notifications,

maintaining status information, calculating technical or operational indicators, organizing records, identifying system events, or performing other functions based on predefined rules or system logic.

Automated processing may also be used to reduce repetitive manual tasks, improve consistency, support operational efficiency, and assist authorized personnel in identifying information requiring attention or review.

The fact that a process is automated does not necessarily mean that the resulting action constitutes an automated decision having legal or similarly significant effects on an individual.

Where automated processing supports a professional, technical, classification, certification, survey, audit, or regulatory determination, the role of human review and professional judgment will depend on the nature of the relevant process and applicable requirements.

13.2 Risk, Security and Fraud Detection

LSR may use automated systems or analytical tools to identify patterns, events, activities, or technical indicators that may suggest unauthorized access, account compromise, fraud, misuse, document manipulation, malicious activity, abnormal system behavior, or other security or operational risks.

Such processing may involve authentication information, IP addresses, session information, device or browser characteristics, access patterns, failed login attempts, user actions, document activity, workflow events, or other relevant technical and operational information.

Automated security systems may generate warnings, risk indicators, alerts, restrictions, or recommendations for further investigation.

Where reasonably appropriate, significant measures affecting a user or organization may be reviewed by authorized personnel before or after action is taken, depending on the nature and urgency of the identified risk.

Nothing in this section prevents LSR from taking immediate automated protective measures, such as blocking a suspicious request, terminating a session, temporarily restricting access, or applying another security control where necessary to protect the Portal, systems, data, users, or services.

13.3 Artificial Intelligence-Assisted Features

LSR may introduce or use artificial intelligence-assisted features to support users, personnel, and operational processes.

Such features may assist with activities including document analysis, information extraction, search, summarization, translation, identification of potentially relevant information, preparation of draft content, classification of records, technical assistance, workflow support, or other functions where artificial intelligence may improve efficiency or usability.

Artificial intelligence-generated or assisted outputs may contain errors, omissions, incomplete information, or other inaccuracies and should not automatically be treated as an authoritative technical, regulatory, classification, certification, legal, or professional determination.

Where an artificial intelligence-assisted feature processes personal data, LSR will seek to limit the information used to what is reasonably necessary for the relevant purpose and apply appropriate access, security, confidentiality, and data protection controls.

Personal data will not be used for unrelated artificial intelligence purposes merely because it is available within LSR systems.

Where LSR uses an external artificial intelligence or technology provider involving the processing of personal data, such processing will be subject to the applicable provisions of this Privacy Policy concerning service providers, international transfers, security, confidentiality, and data protection.

13.4 Human Review and Decision-Making

LSR recognizes the importance of appropriate human involvement in decisions involving professional judgment, technical assessment, classification, certification, survey, audit, regulatory matters, or other activities where human review is required by the nature of the service or applicable requirements.

Automated systems and artificial intelligence may provide information, indicators, recommendations, drafts, alerts, calculations, or other forms of assistance to authorized personnel without replacing the professional responsibility of the person responsible for the relevant determination.

Where a decision is not intended to be made solely by automated means, authorized personnel should retain meaningful ability to review relevant information, consider the circumstances, assess automated outputs, and make or confirm the appropriate determination.

Where solely automated decision-making producing legal or similarly significant effects is used and falls within applicable legal requirements, LSR will provide the protections required under applicable law, which may include opportunities for human intervention, expression of the individual's position, review, or contesting the decision where applicable.

The level and form of human review may vary according to the nature, risk, significance, and legal or professional requirements of the relevant process.

14. Your Privacy Rights

Depending on the applicable data protection law, individuals may have certain rights regarding personal data processed by LSR.

The availability, scope, conditions, and limitations of these rights may vary according to the jurisdiction, the nature of the processing, the legal basis relied upon, the category of personal data involved, and applicable legal, regulatory, certification, professional, or other requirements.

LSR will assess requests concerning personal data in accordance with the data protection law applicable to the relevant processing activity. The existence of a right under one jurisdiction does not necessarily mean that the same right applies in the same manner to all individuals or processing activities.

The exercise of a data protection right does not automatically require LSR to delete, modify, restrict, transfer, or cease processing information where continued processing is required or permitted by applicable law or is necessary for legal, regulatory, certification, audit, security, or other lawful purposes.

14.1 Right of Access

Where provided by applicable law, individuals may have the right to request confirmation as to whether LSR processes personal data relating to them and to request access to such personal data and associated information.

Depending on applicable law, this may include information concerning the purposes of processing, categories of personal data, categories of recipients, applicable retention periods or criteria, sources of information, international transfers, and other information required by law.

LSR may require sufficient information to identify the individual, locate the relevant records, determine the scope of the request, and protect personal data from unauthorized disclosure.

Access may be limited or refused where permitted or required by applicable law, including where disclosure would adversely affect the rights and freedoms of others, confidentiality obligations, privileged information, security, investigations, or other protected interests.

Where a document or record contains personal data relating to multiple individuals, LSR may redact, restrict, separate, or otherwise protect information relating to other persons before responding to an access request.

14.2 Right to Rectification

Where provided by applicable law, individuals may request correction of inaccurate personal data relating to them and, where appropriate, completion of incomplete personal data.

LSR may request supporting information or documentation where reasonably necessary to verify the accuracy of a requested correction.

A correction to current personal data does not necessarily require alteration or deletion of historical records that accurately reflect information, decisions, submissions, approvals, certificates, survey findings, audit records, or other circumstances as they existed at the relevant time.

Where necessary to preserve record integrity and traceability, LSR may correct information by recording an amendment, updated version, supplementary record, or other appropriate mechanism rather than altering the original historical record.

14.3 Right to Erasure

Where provided by applicable law, individuals may have the right to request deletion of personal data in certain circumstances.

A request for erasure does not create an absolute right to deletion. LSR may continue to retain and process personal data where retention or processing is required or permitted by applicable law or is necessary for legal obligations, regulatory requirements, statutory or certification functions,

establishment or defence of legal claims, security, fraud prevention, audit, record integrity, or other lawful purposes.

In particular, information forming part of vessel histories, certificates, survey or audit records, technical decisions, approvals, regulatory records, security logs, or other records requiring historical integrity or traceability may need to be retained notwithstanding an erasure request.

Where only part of the relevant information must continue to be retained, LSR may delete, anonymize, restrict, separate, or otherwise limit processing of information that is no longer necessary while retaining information for which a lawful retention basis remains.

Where LSR cannot comply fully or partially with an erasure request, LSR may provide information regarding the applicable reason or legal basis where required by applicable law.

14.4 Right to Restriction of Processing

Where provided by applicable law, individuals may have the right to request restriction of processing of their personal data in certain circumstances.

Restriction may apply, for example, while the accuracy of personal data is being verified, while an objection is being assessed, or where applicable law otherwise requires processing to be temporarily or permanently limited.

Where processing is restricted, LSR may continue to store the relevant personal data and may process it where permitted by applicable law, including for the establishment, exercise, or defence of legal claims, protection of the rights of another person, important public interests, security, or other legally recognized purposes.

Restriction of processing does not necessarily require deletion of the underlying records.

14.5 Right to Data Portability

Where provided by applicable law and where the applicable legal conditions are satisfied, individuals may have the right to receive certain personal data concerning them in a structured, commonly used, and machine-readable format and to transmit that information to another controller.

This right generally applies only to categories of personal data and processing activities covered by the relevant law and does not necessarily apply to all records maintained by LSR.

The right to data portability does not necessarily require LSR to provide complete documents, certificates, reports, audit trails, technical records, proprietary information, information concerning other individuals, or records whose integrity must be preserved.

Where technically feasible and legally required, LSR may transmit eligible personal data directly to another controller at the individual's request.

14.6 Right to Object

Where provided by applicable law, individuals may have the right to object to certain processing of their personal data, including processing based on legitimate interests or other legal bases for which a right to object is recognized.

Where an objection is made, LSR will assess the request in accordance with applicable law, the legal basis for processing, the reasons for the objection, and the grounds requiring or permitting continued processing.

LSR may continue processing where applicable law permits it to demonstrate compelling legitimate grounds that override the individual's interests, rights, and freedoms, or where processing is necessary for the establishment, exercise, or defence of legal claims or another legally recognized purpose.

An objection will not prevent processing that is independently required by a legal or regulatory obligation or supported by another applicable lawful basis.

14.7 Rights Relating to Automated Decision-Making

Where applicable law provides such rights, individuals may have rights concerning decisions based solely on automated processing that produce legal effects or similarly significant effects concerning them.

LSR may use automated systems to support workflow routing, security monitoring, validation, risk identification, prioritization, analytics, or other operational functions.

The use of automation to assist personnel, identify information, generate alerts, calculate indicators, or recommend an action does not necessarily constitute solely automated decision-making where a meaningful human review or decision remains part of the process.

Where LSR implements solely automated decision-making that falls within applicable legal restrictions, LSR will apply the safeguards and provide the rights required by applicable law.

14.8 Withdrawal of Consent

Where LSR processes personal data on the basis of consent, individuals may withdraw their consent at any time, subject to applicable law.

Withdrawal of consent will not affect the lawfulness of processing carried out on the basis of consent before its withdrawal.

Withdrawal will also not require LSR to cease processing where the same or related personal data must continue to be processed under another applicable legal basis, including legal obligations, contractual requirements, legitimate interests, certification requirements, security, or legal claims.

Where withdrawal affects an optional feature, communication, or processing activity, the relevant feature or service may no longer be available to the individual.

14.9 Right to Lodge a Complaint

Where provided by applicable law, individuals may have the right to lodge a complaint with the competent data protection, supervisory, regulatory, or other authority regarding the processing of their personal data.

The competent authority may depend on the individual's location, the establishment responsible for the relevant processing, the jurisdiction in which the processing occurs, or other criteria established by applicable law.

Individuals may contact LSR regarding their concerns before making a complaint to an authority, although doing so does not limit any right to approach a competent authority directly where applicable law provides such a right.

LSR will cooperate with competent authorities in accordance with applicable legal obligations.

14.10 Exercising Your Rights

Requests concerning personal data rights may be submitted to LSR using the contact details specified in this Privacy Policy or through any dedicated privacy request mechanism made available by LSR.

A request should contain sufficient information to enable LSR to identify the individual, understand the right being exercised, determine the relevant personal data or processing activity, and respond appropriately.

LSR may request additional information or reasonable proof of identity where necessary to verify the identity and authority of the person making the request and to prevent unauthorized access, alteration, disclosure, or deletion of personal data.

Where a request is made on behalf of another individual, LSR may require evidence that the person making the request is authorized to act on that individual's behalf.

LSR will respond within the period required by applicable law. Where permitted, the response period may be extended where a request is complex or multiple requests have been submitted, subject to any applicable notification requirements.

Where permitted by applicable law, LSR may refuse or impose a reasonable charge for requests that are manifestly unfounded, excessive, repetitive, or otherwise subject to a lawful limitation.

15. Third-Party Services and External Links

LSR may use, integrate with, reference, or provide access to third-party services, platforms, websites, applications, databases, communication tools, infrastructure providers, verification services, or other external resources in connection with the Portal and LSR services.

Third-party services may be used to support functionality such as hosting, communications, authentication, verification, analytics, technical infrastructure, external information access, document exchange, or other operational purposes.

Where a third party processes personal data on behalf of LSR, such processing may be subject to contractual, confidentiality, security, and data protection requirements appropriate to the nature of the service.

Where a third party independently determines the purposes and means of processing personal data, its own privacy policy, terms, and data protection practices may apply to the relevant processing.

The inclusion of, access to, or integration with a third-party service or external resource does not necessarily mean that LSR controls or is responsible for all processing activities carried out independently by that third party.

15.1 Third-Party Platforms and Services

LSR may rely on third-party platforms, software, infrastructure, service providers, or technology partners to support the operation and delivery of the Portal and related services.

These may include hosting providers, communication services, email delivery services, identity or verification providers, analytics tools, technical infrastructure providers, backup or storage services, cybersecurity services, external databases, or other technology and operational service providers.

Where such providers process personal data on behalf of LSR, LSR may require appropriate contractual terms addressing confidentiality, security, permitted processing, retention, incident management, international transfers, subcontracting, and deletion or return of personal data.

Where a third-party platform or service is used by the user independently or provides services directly to the user, the processing of personal data may also be governed by that provider's own terms and privacy practices.

LSR does not represent that all third-party services used in connection with the Portal are identical in their privacy, security, or technical practices.

15.2 External Websites and Links

The Portal or LSR communications may contain links to external websites, portals, databases, services, documents, or other resources operated by third parties.

Such links may be provided for convenience, reference, verification, regulatory access, technical information, operational support, or other legitimate purposes.

When a user follows an external link or accesses a third-party website or service, that third party may collect or process personal data independently from LSR.

LSR does not control the privacy practices, security measures, content, availability, or data processing activities of external websites or services that are not operated by or on behalf of LSR.

Users are encouraged to review the privacy policies, terms of use, cookie notices, and other relevant information provided by the operator of an external website or service before submitting personal data or using that service.

The presence of an external link within the Portal does not, by itself, constitute endorsement of the privacy, security, accuracy, legality, or practices of the external resource.

15.3 Third-Party Privacy Practices

Third parties that receive, collect, or process personal data independently from LSR may be responsible for their own compliance with applicable data protection laws.

Where a third party acts as an independent controller or otherwise determines its own processing purposes and methods, LSR may not have authority to control how that third party uses, retains, transfers, discloses, or otherwise processes personal data.

LSR will seek to engage appropriate service providers and business partners where their activities involve personal data processed on behalf of LSR, taking into account the nature of the service and reasonably available information concerning data protection and security practices.

However, where a user independently chooses to provide personal data to a third party or access an independently operated service, that third party's privacy practices will generally govern the relevant processing.

Nothing in this section limits LSR's responsibilities for personal data processing activities for which LSR is responsible under applicable law.

16. Children's Privacy

The Portal and LSR services are intended for professional, commercial, regulatory, classification, certification, and other maritime-related activities and are not directed to children.

LSR does not knowingly provide Portal accounts or professional access to individuals who do not satisfy the applicable age, legal capacity, professional, or authorization requirements relevant to the service.

However, in limited circumstances, personal data relating to children may be contained in documents, records, declarations, supporting materials, emergency information, family-related records, or other information submitted to LSR as part of a lawful maritime, employment, regulatory, legal, or administrative process.

Where personal data relating to a child is processed, LSR will seek to limit such processing to what is relevant and reasonably necessary for the applicable purpose and to apply any additional protections required under applicable law.

16.1 Age Restrictions

The Portal is intended for individuals who are legally capable of acting in a professional or authorized capacity in connection with LSR services.

Users must satisfy any age, legal capacity, employment, professional, contractual, or authorization requirements applicable to their role or activity within the Portal.

LSR may refuse, restrict, suspend, or terminate access where it determines that an individual does not satisfy the applicable requirements for Portal use or professional participation.

Where a user acts on behalf of an organization, the organization is responsible for ensuring that the individual is appropriately authorized and legally capable of performing the relevant actions.

Nothing in this section is intended to impose a specific universal minimum age where applicable law or the relevant professional activity establishes a different requirement.

16.2 Unintentional Collection of Children's Data

LSR does not intentionally seek to collect personal data from children for general Portal registration, account administration, marketing, analytics, or routine professional services.

If LSR becomes aware that personal data relating to a child has been collected or submitted unnecessarily, without an appropriate purpose, or in circumstances where the processing is not lawful, LSR may take appropriate steps to delete, restrict, return, redact, anonymize, or otherwise secure the information.

Before deleting or altering such information, LSR may assess whether the data forms part of a legal, regulatory, certification, employment, safety, emergency, evidentiary, or other record that must be preserved.

Where the information must be retained for a lawful purpose, LSR may restrict access, minimize further processing, apply additional safeguards, or retain only the information necessary for that purpose.

Organizations and users submitting information to LSR should avoid including personal data relating to children unless such information is relevant and reasonably necessary for the applicable service, legal obligation, regulatory requirement, or other lawful purpose.

Where applicable law requires consent, authorization, notice, or another specific condition for processing a child's personal data, the party responsible for providing the information to LSR must ensure that the relevant requirement has been satisfied, unless responsibility for that requirement rests directly with LSR under applicable law.

17. Changes to this Privacy Policy

LSR may review, amend, update, or replace this Privacy Policy from time to time to reflect changes in applicable laws or regulations, LSR services and operations, Portal functionality, technologies, data processing activities, security practices, organizational arrangements, regulatory requirements, or other relevant circumstances.

The current version of this Privacy Policy will be made available through the Portal or other appropriate means and will indicate the applicable effective date, last updated date, version number, or other revision information where appropriate.

Changes to this Privacy Policy do not, by themselves, provide a legal basis for processing personal data in a manner that would otherwise be unlawful. Where a change to LSR's processing activities

requires a new legal basis, consent, notice, authorization, or other measure under applicable law, LSR will take the required steps before or in connection with the relevant processing.

Individuals are encouraged to review this Privacy Policy periodically to remain informed about how LSR processes and protects personal data.

17.1 Policy Updates

LSR may update this Privacy Policy where necessary or appropriate to reflect developments affecting the processing of personal data.

Updates may include changes resulting from new or amended legal requirements, regulatory guidance, classification or certification activities, new Portal features, changes to existing services, new technologies, changes in service providers, international operations, security practices, organizational changes, or modifications to the categories, purposes, or methods of personal data processing.

Minor changes may include editorial corrections, formatting changes, clarifications, updated contact information, or other modifications that do not materially alter the nature of personal data processing.

Material changes may include changes that significantly affect the categories of personal data processed, purposes of processing, legal bases, categories of recipients, international transfers, retention practices, use of automated processing, or the rights and choices available to individuals.

LSR may maintain previous versions or revision records of this Privacy Policy where appropriate for governance, compliance, audit, or historical purposes.

17.2 Material Changes

Where changes to this Privacy Policy or the underlying processing activities are material, LSR may provide notice through the Portal, account notifications, email, prominent notices, or other appropriate communication methods.

The method and timing of notification may depend on the significance of the change, the nature of the processing affected, the available contact information, and applicable legal requirements.

Where applicable law specifically requires prior notice, renewed consent, authorization, or another action before a material change may take effect for particular processing activities, LSR will take the required measures.

Continued use of the Portal following an update to this Privacy Policy will not be treated as consent to processing where applicable law requires specific, informed, or affirmative consent.

Users remain responsible for ensuring that contact information associated with their accounts is accurate and current so that relevant notices can be delivered where appropriate.

17.3 Effective Date and Version History

Each version of this Privacy Policy may identify its effective date, last updated date, version or revision number, and other information reasonably necessary to distinguish it from previous versions.

Unless otherwise stated or required by applicable law, an updated Privacy Policy will become effective on the date specified in the updated version.

Where different provisions become effective at different times due to legal, regulatory, technical, or operational requirements, LSR may identify the applicable effective dates separately.

LSR may maintain a version history or revision record identifying previous versions and, where appropriate, a summary of material changes.

Historical versions may be retained for legal, compliance, governance, audit, evidentiary, or reference purposes.

18. Contact Us

Individuals, users, organizations, and other relevant parties may contact LSR regarding this Privacy Policy, the processing of personal data, the exercise of applicable data protection rights, or other privacy-related questions or concerns.

Privacy-related communications may include requests for information, access, rectification, erasure, restriction, objection, withdrawal of consent, data portability, complaints, questions concerning international transfers, or reports concerning the security or inappropriate disclosure of personal data.

LSR will review privacy-related communications in accordance with applicable data protection laws and the nature of the request.

Where a request concerns a specific account, organization, vessel, application, survey, audit, certificate, document, or other LSR record, sufficient information should be provided to enable LSR to identify the relevant processing activity and respond appropriately.

18.1 Privacy Enquiries

Questions regarding this Privacy Policy or LSR's processing of personal data may be submitted using the contact information provided below.

When contacting LSR, individuals should provide sufficient information to explain the nature of their enquiry without unnecessarily providing additional personal data or sensitive information.

Where necessary to respond to an enquiry, LSR may request additional information to identify the relevant processing activity, account, record, organization, vessel, service, or other matter concerned.

General privacy enquiries do not require individuals to provide passwords, authentication credentials, verification codes, or other confidential account-security information. LSR should not be provided with such information through ordinary email communications.

18.2 Data Protection Requests

Individuals seeking to exercise a data protection right should clearly identify the nature of the request and provide sufficient information to enable LSR to locate the relevant personal data.

LSR may require reasonable verification of identity before processing a request where necessary to protect personal data against unauthorized access, disclosure, modification, or deletion.

The information requested for identity verification will be limited, where reasonably practicable, to what is necessary to verify the identity or authority of the requester.

Where a request is submitted by an authorized representative, LSR may require appropriate evidence demonstrating the representative's authority to act on behalf of the relevant individual.

Requests will be assessed and responded to within the timeframe required by applicable law, subject to any lawful extensions, exemptions, limitations, or additional verification requirements.

Submitting a data protection request does not require LSR to take an action that would conflict with applicable legal, regulatory, certification, security, audit, record-keeping, or other lawful obligations.

18.3 Complaints and Regulatory Matters

Privacy-related enquiries and requests may be directed to LSR using the following contact details:

- Life At Sea Register (LSR)
- Website: lsregister.com
- Email: support@lsregister.com

LSR may establish a dedicated privacy or data protection contact address or request mechanism. Where such a mechanism is made available, the current contact information will be published through the Portal or this Privacy Policy.

Where correspondence relates to the exercise of a data protection right, individuals should indicate that the communication concerns a privacy or data protection request so that it can be directed to the appropriate personnel.

Contact information may be updated from time to time. The current contact information published by LSR should be used when submitting privacy-related communications.

Appendix A — Categories of Personal Data and Processing Purposes

This Appendix provides an overview of the principal categories of personal data that LSR may process and the purposes for which such information may be used.

The categories and examples described below are illustrative and may vary depending on the relevant individual, organization, vessel, service, application, survey, audit, certification activity, regulatory requirement, Portal functionality, or other circumstances.

A particular item of personal data may fall within more than one category and may be processed for more than one purpose where an appropriate legal basis exists.

Not every category of personal data described in this Appendix will be collected or processed in relation to every individual or LSR service.

This Appendix should be read together with the main provisions of this Privacy Policy, including the sections concerning the categories of personal data processed, purposes and legal bases of processing, sharing and disclosure, international transfers, retention, security, and individual rights.

A.1 Identity and Identification Data

Examples of personal data

Identity and identification data may include:

- Full name;
- Given name and surname;
- Date of birth;
- Nationality;
- Gender, where relevant and lawfully required;
- Photograph;
- Signature;
- Passport or travel document information;
- National identification information;
- Seafarer identification information;
- Professional identification numbers;
- User, applicant, surveyor, auditor, representative, or other LSR identifiers;
- Copies or details of official identification documents where necessary.

Processing purposes

LSR may process identity and identification data for purposes including:

- Identifying individuals;
- Creating and administering Portal accounts;
- Identity verification;
- Verifying authority to act on behalf of an organization or vessel;
- Classification and certification activities;
- Survey, audit, inspection, and technical review processes;
- Issuing, maintaining, verifying, endorsing, renewing, suspending, withdrawing, or otherwise administering certificates and records;
- Including required identity information in certificates, reports, forms, records, or other official documents;

- Regulatory and statutory compliance;
- Communication with flag administrations and competent authorities;
- Fraud prevention and security;
- Maintaining accurate and traceable professional records

A.2 Contact Data

Examples of personal data

Contact data may include:

- Email address;
- Telephone or mobile number;
- Business contact details;
- Mailing or correspondence address;
- Organizational contact information;
- Preferred communication information;
- Other contact information voluntarily provided in connection with LSR services.

Processing purposes

LSR may process contact data for:

- Account administration;
- Service communications;
- Application and request management;
- Survey and audit coordination;
- Certificate and document administration;
- Notifications and alerts;
- Verification communications;
- Responding to enquiries and support requests;
- Communicating regarding regulatory, operational, contractual, technical, or security matters;
- Exercising data protection rights;
- Maintaining appropriate contact with authorized representatives.

A.3 Account and Access Data

Examples of personal data

Account and access data may include:

- User account identifier;
- Username;
- Organizational affiliation;
- User role;
- Access permissions;
- Account status;
- Authentication and verification records;
- Login and logout information;
- Session information;
- Password-related security information stored in protected form;
- Multi-factor authentication information where implemented;
- Account creation and modification history.

Processing purposes

LSR may process this information for:

- Creating and maintaining user accounts;
- Authentication;
- Authorization and access control;
- Managing organizational relationships and roles;
- Providing Portal functionality;
- Protecting accounts and systems;
- Detecting unauthorized or suspicious access;
- Maintaining audit trails;
- Investigating security incidents;
- Enforcing applicable access restrictions;
- Supporting operational accountability and traceability.

A.4 Professional and Qualification Data

Examples of personal data

Professional and qualification data may include:

- Job title;
- Position or role;
- Employer or organizational affiliation;
- Professional experience;
- Curriculum vitae;
- Certificates of competency;
- Licenses;
- Qualifications;
- Training records;
- Examination or assessment information;
- Professional approvals or authorizations;
- Surveyor or auditor qualifications;
- Scope of authorization;
- Professional history relevant to LSR services.

Processing purposes

LSR may process professional and qualification data for:

- Verifying professional competence;
- Assessing eligibility for roles or authorizations;
- Surveyor, auditor, inspector, or other professional approval processes;
- Assigning appropriate duties and permissions;
- Classification and certification activities;
- Compliance with regulatory or professional requirements;
- Training, assessment, examination, and authorization;
- Maintaining professional records;
- Demonstrating competence to flag administrations, authorities, clients, or other authorized parties where required.

A.5 Organisation and Relationship Data

Examples of personal data

This category may include personal data relating to an individual's relationship with:

- Shipowners;
- Managers;
- Operators;
- DOC holders;
- Bareboat charterers;
- Agents;
- Employers;
- Service providers;
- Authorized representatives;
- Other organizations participating in an LSR process.

It may also include role, authority, relationship status, organizational permissions, appointment information, and records demonstrating the individual's authority to act.

Processing purposes

LSR may process this information for:

- Establishing organizational relationships;
- Verifying authority and representation;
- Managing Portal access;
- Assigning roles and permissions;
- Determining access to vessels, requests, documents, certificates, or workflows;
- Coordinating services between relevant parties;
- Maintaining accountability;
- Supporting contractual, regulatory, classification, and certification processes.

A.6 Vessel, Survey, Audit and Certification Data

Personal data may be contained in records relating to vessels and professional maritime activities.

Examples of personal data

Such information may include:

- Names, roles, signatures, and professional details of masters, officers, crew members, surveyors, auditors, inspectors, representatives, reviewers, or approving personnel;
- Survey and audit attendance information;
- Findings, observations, corrective actions, comments, and professional assessments associated with identifiable individuals;
- Certificate information;
- Signatory and approval information;
- Vessel-related correspondence;
- Applications and supporting documents;
- Records concerning classification or statutory services;
- Information contained in forms, reports, checklists, declarations, and technical submissions.

Processing purposes

- Classification;
- Statutory certification;
- Surveys, audits, and inspections;
- Technical review and approval;
- Certificate issuance and verification;
- Maintaining vessel and certification history;
- Regulatory reporting;
- Compliance monitoring;
- Transfer of class;
- Corrective action management;
- Maintaining professional accountability and traceability;
- Responding to flag administrations, port state authorities, and other competent authorities;
- Investigations, disputes, claims, or other lawful professional purposes.

A.7 Documents and Communications Data

Examples of personal data

This category may include personal data contained in:

- Emails;
- Portal messages;
- Support communications;
- Applications;
- Requests;
- Comments;
- Clarification responses;
- Uploaded documents;
- Forms;
- Reports;
- Correspondence;
- Notifications;
- Attachments;
- Records of communications with LSR personnel, surveyors, auditors, organizations, or authorities.

Processing purposes

- providing and administering services;
- Responding to enquiries;
- Managing applications and requests;
- Conducting reviews;
- Coordinating surveys and audits;
- Maintaining records of decisions and instructions;
- Supporting workflow processes;
- Resolving disputes or clarifications;
- Compliance, audit, legal, and evidentiary purposes;
- Maintaining operational continuity and traceability.

A.8 Technical, Device and Usage Data

Examples of personal data

Technical and usage information may include:

- IP address;
- Browser type and characteristics;
- Operating system;
- Device type;
- Screen or display information;
- Session information;
- Login activity;
- Access timestamps;
- Page visits;
- Navigation paths;
- Feature usage;
- Referrer information;
- Performance information;
- Error records;
- Security events;
- Technical identifiers;
- Other system or usage metadata.

Processing purposes

LSR may process this information for:

- Operating and maintaining the Portal;
- Authentication and session management;
- Security monitoring;
- Detecting unauthorized access, abuse, or suspicious activity;
- Troubleshooting;
- Performance analysis;
- Improving Portal functionality;

- Maintaining audit trails;
- Analytics where permitted;
- Investigation of security or operational incidents;
- Compliance and evidentiary purposes.

A.9 Browser Storage and Form Progress Data

Examples of personal data or related information

LSR may store information through local storage, session storage, cookies, or similar technologies, including:

- Form progress;
- Temporary draft information;
- Workflow state;
- Navigation context;
- Session information;
- User preferences;
- Information required to restore an incomplete process;
- Technical identifiers associated with the relevant functionality.

Processing purposes

Such information may be processed for:

- Providing Save & Exit functionality;
- Allowing users to return to incomplete forms;
- Restoring intentionally saved information;
- Maintaining workflow continuity;
- Preserving user preferences;
- Maintaining authentication or session functionality;
- Providing security and other essential Portal functions.

The information stored through browser technologies will depend on the relevant implementation and should be limited to information reasonably necessary for the applicable functionality.

A.10 Security, Audit and Compliance Data

Examples of personal data

This category may include:

- Audit logs;
- User identifiers;
- Access records;
- Authentication events;
- Failed login attempts;
- Permission changes;
- Administrative actions;
- Workflow actions;
- Document access and modification records;
- Security alerts;
- Suspicious activity indicators;
- Incident records;
- Investigation records;
- Compliance review information.

Processing purposes

- Information security;
- Access control;
- Fraud and misuse prevention;
- Detecting and investigating incidents;
- Maintaining accountability;
- Preserving system and record integrity;
- Audit and compliance;
- Regulatory requirements;
- Resolving disputes;
- Establishing, exercising, or defending legal claims;
- Maintaining evidence and operational traceability.

A.11 Sensitive and Special Category Data

LSR does not ordinarily require sensitive or specially protected personal data for general Portal use. However, such information may be processed in limited circumstances as described in this Privacy Policy.

Examples may include:

- Health or medical information where relevant to a lawful maritime, fitness, safety, employment, or regulatory process;
- Biometric information where used for identification and lawfully processed;
- Sensitive information appearing incidentally in official documents or submitted records;
- Other categories receiving enhanced protection under applicable law.

Processing purposes may include:

- Compliance with legal or regulatory requirements;
- Maritime safety or fitness requirements;
- Verification of legally required documentation;
- Professional or regulatory processes;
- Protection of individuals or other persons;
- Establishment, exercise, or defence of legal claims;
- Other purposes permitted or required by applicable law.

Processing of such information will be subject to any additional conditions and safeguards required under applicable law.

A.12 Data Relating to Children

LSR services are not directed to children. However, personal data relating to children may occasionally appear within records submitted for legitimate maritime, legal, employment, safety, emergency, family-related, or administrative purposes.

Such information may be processed for:

- Compliance with applicable legal or regulatory requirements;
- Emergency or safety-related purposes;
- Administration of relevant lawful records;
- Other purposes for which processing is necessary and legally permitted.

Where such data is not necessary or has been submitted without an appropriate lawful purpose, LSR may delete, redact, restrict, return, anonymize, or otherwise appropriately manage the information in accordance with Section 16 of this Privacy Policy.

A.13 Artificial Intelligence and Automated Processing Data

Where LSR uses automated or artificial intelligence-assisted functionality, relevant personal data may be processed as input, contextual information, metadata, or information associated with the resulting output.

Relevant information may include:

- Information contained in documents submitted for analysis;
- Workflow and application information;
- Technical and operational information;
- Search queries or instructions;
- Security indicators;
- Information extracted or classified by automated systems;
- Records of automated outputs or subsequent human review.

Processing purposes may include:

- Workflow support;
- Document analysis;
- Information extraction;
- Search and retrieval;
- Summarization or translation;
- Validation;
- Risk or security identification;
- Technical assistance;
- Supporting authorized personnel in review and decision-making;
- Improving operational efficiency where lawfully permitted.

The processing of personal data through automated or artificial intelligence-assisted systems remains subject to the applicable provisions of this Privacy Policy and applicable law.

Appendix B — Data Retention Framework

This Appendix describes the general framework applied by LSR when determining how long personal data and records containing personal data may be retained.

Retention periods may vary depending on the category of information, purpose of processing, nature of the relevant service or relationship, applicable legal or regulatory requirements, classification and certification obligations, contractual requirements, security needs, limitation periods, audit requirements, and the need to maintain accurate and traceable historical records.

LSR does not necessarily retain all personal data for the same period. Information may be deleted, anonymized, restricted, archived, or otherwise managed when it is no longer reasonably necessary for the purposes for which it is retained, subject to applicable legal and operational requirements.

The categories and retention criteria described in this Appendix are intended as a general framework and do not establish a fixed retention period where a different period is required or permitted by applicable law, a competent authority, a flag administration, contractual obligations, professional requirements, or the nature of the relevant record.

B.1 Account and User Profile Data

Relevant records may include:

- Account information;
- User profile information;
- Contact details;
- Organizational affiliation;
- Roles and permissions;
- Account verification information;
- Account status and administrative history.

General retention approach

Such information may be retained for the duration of the user's active account, organizational relationship, authorization, or other relevant relationship with LSR.

Following account closure, termination of authorization, or the end of the relevant relationship, LSR may retain information for an additional period where necessary for legal compliance, security, dispute resolution, audit, fraud prevention, record integrity, or other legitimate purposes.

Information that is no longer required may be deleted, anonymized, archived, or restricted in accordance with applicable requirements.

Closing or deleting a Portal account does not necessarily result in deletion of personal data contained in independent classification, certification, survey, audit, regulatory, contractual, security, or historical records.

B.2 Applications, Requests and Workflow Records

Relevant records may include:

- Applications;
- Service requests;
- Request threads;
- Workflow events;
- Actions and approvals;
- Clarifications;
- Submissions;
- Supporting documents;
- Status histories;
- Change requests;
- Related communications.

General retention approach

Records associated with applications, requests, and workflows may be retained throughout the relevant process and for an appropriate period after completion, cancellation, rejection, withdrawal, or closure.

Retention after closure may be necessary to maintain evidence of submissions, decisions, approvals, instructions, communications, contractual activities, regulatory compliance, or the history of services provided by LSR.

Where a workflow forms part of a classification, certification, statutory, survey, audit, or other professional record, the relevant information may be retained together with or for the same period as the associated professional record.

B.3 Classification and Vessel Records

Relevant records may include:

- Vessel particulars and histories;
- Classification status;
- Technical reviews;
- Approvals;
- Survey records;
- Conditions, recommendations, memoranda, or similar records;

- Transfer of class information;
- Classification decisions;
- Supporting technical documents;
- Associated correspondence and approval histories.

General retention approach

Classification and vessel records may require long-term or historical retention to preserve continuity, traceability, technical history, professional accountability, and evidence of classification decisions.

Such records may therefore be retained after the end of a vessel's active relationship with LSR, transfer of class, suspension, withdrawal, deletion from class, change of ownership or management, or other change in status.

Retention will be determined according to applicable classification requirements, professional obligations, legal and regulatory requirements, contractual requirements, limitation periods, historical record requirements, and the nature of the information concerned.

Where personal data forms part of a classification record whose integrity must be preserved, the termination of an individual's account or organizational relationship does not necessarily require removal of that personal data from the historical record.

B.4 Statutory Certification Records

Relevant records may include:

- Statutory certificates;
- Interim, short-term, full-term, or other certificates;
- Endorsements;
- Survey and audit records;
- Applications;
- Approvals;
- Supporting evidence;
- Flag authorization information;
- Correspondence with flag administrations;
- Certificate issuance, renewal, suspension, withdrawal, cancellation, and verification records.

General retention approach

Statutory certification records may be retained for periods required by applicable conventions, codes, laws, flag administrations, competent authorities, authorization agreements, recognized organization requirements, or other applicable regulatory obligations.

LSR may also retain historical certificate records after expiration, replacement, withdrawal, cancellation, or invalidation where necessary to demonstrate the status and history of certification at a particular time.

Personal data appearing in certificates or supporting statutory records may therefore remain within historical records where necessary to preserve authenticity, integrity, accountability, or regulatory traceability.

B.5 Survey, Audit and Inspection Records

Relevant records may include:

- Survey reports;
- Audit reports;
- Inspection records;
- Checklists;
- Findings;
- Non-conformities;
- Observations;
- Corrective actions;
- Evidence and supporting documents;
- Attendance records;
- Signatures;
- Photographs where applicable;
- Communications and review records.

General retention approach

These records may be retained for the period necessary to support classification, certification, statutory compliance, professional accountability, subsequent surveys or audits, investigations, disputes, and historical traceability.

Where the records support a certificate, classification status, statutory service, or regulatory determination, their retention may correspond to or exceed the active validity period of the relevant certificate or service.

Historical records may be retained where necessary to demonstrate what was inspected, identified, reported, corrected, approved, or decided at a particular time.

B.6 Professional Qualification and Authorization Records

Relevant records may include:

- CVs;
- Qualifications;
- Licenses;
- Certificates of competency;
- Training records;
- Examination results;
- Assessments;
- Authorization scope;
- Approval history;
- Surveyor or auditor performance and professional records.

General retention approach

Such records may be retained while the individual remains authorized, approved, employed, contracted, registered, or otherwise professionally associated with LSR.

Relevant records may continue to be retained after the professional relationship ends where necessary to demonstrate historical competence, authorization, assignments, decisions, surveys, audits, approvals, regulatory compliance, or professional accountability.

Information that no longer serves a lawful or necessary purpose may be deleted, anonymized, archived, or restricted as appropriate.

B.7 Communications and Support Records

Relevant records may include:

- Emails;
- Portal messages;
- Support requests;
- Clarifications;
- Notifications;
- Correspondence;

- Complaints;
- Privacy enquiries;
- Communications concerning applications, services, surveys, audits, certificates, or technical matters.

General retention approach

Communications may be retained for the period necessary to resolve the relevant matter and subsequently where required to maintain evidence, operational continuity, service history, compliance, contractual records, or legal claims.

Communications forming part of another professional or regulatory record may be retained according to the retention requirements applicable to that record.

Routine communications with no continuing operational, legal, regulatory, security, or historical value may be deleted in accordance with LSR's applicable retention practices.

B.8 Security and Audit Records

Relevant records may include:

- Authentication logs;
- Login history;
- Access logs;
- Session records;
- Administrative actions;
- Permission changes;
- Audit trails;
- Security alerts;
- Suspicious activity indicators;
- Incident records;
- Investigation records.

General retention approach

Security and audit records may be retained for periods reasonably necessary to detect and investigate incidents, protect systems and accounts, maintain accountability, demonstrate compliance, resolve disputes, prevent fraud or abuse, and establish or defend legal claims.

Different security records may have different retention periods depending on their sensitivity, operational usefulness, storage requirements, security risks, and applicable legal obligations.

Records associated with an identified security incident, investigation, legal matter, or regulatory requirement may be retained for longer than routine technical logs.

B.9 Cookies, Local Storage and Temporary Data

Relevant information may include:

- Cookies;
- Local storage;
- Session storage;
- Authentication state;
- User preferences;
- Form progress;
- Temporary draft data;
- Save & Exit information;
- Workflow state;
- Navigation context;
- Other temporary browser or session information.

General retention approach

Retention depends on the nature and purpose of the technology used.

Session-based information may be removed when the relevant session ends, while persistent information may remain for a defined period or until it is replaced, deleted, expires, or is removed by the user.

Information stored through local storage for **Save & Exit**, form recovery, draft preservation, or workflow continuity may remain on the user's device for the period necessary to support the relevant functionality.

Where a submitted or finalized form becomes part of an LSR record, the information submitted to LSR may subsequently be retained under the retention framework applicable to that record independently of any browser-stored copy.

Users may delete locally stored information through their browser or device controls, but doing so may cause saved progress, drafts, preferences, or other functionality to be lost.

LSR may establish expiry mechanisms or other controls for browser-stored information where appropriate to reduce unnecessary retention.

B.10 Analytics and Technical Usage Data

Relevant records may include:

- Page views;
- Session activity;
- Device and browser information;
- IP addresses;
- Referrer information;
- Performance metrics;
- Error information;
- Feature usage;
- Other technical analytics data.

General retention approach

Analytics and technical usage information may be retained for periods reasonably necessary for performance analysis, service improvement, security, troubleshooting, statistical analysis, and other lawful purposes.

Where detailed identifiable information is no longer necessary, LSR may aggregate, de-identify, or anonymize information and retain the resulting non-personal or anonymized information for longer-term statistical, operational, historical, or analytical purposes.

Retention of identifiable analytics data may be shorter than retention of aggregated or anonymized information.

B.11 Privacy Requests and Consent Records

Relevant records may include:

- Data protection requests;
- Identity verification associated with a request;
- Responses and correspondence;
- Consent records;
- Consent withdrawals;
- Cookie or technology preferences where recorded;
- Objections;
- Complaints;
- Records demonstrating LSR's response or compliance.

General retention approach

Such records may be retained after completion of the relevant request or withdrawal where necessary to demonstrate compliance with applicable data protection requirements, establish what action was requested and taken, resolve disputes, or defend legal claims.

Information collected solely to verify identity for a privacy request should not be retained longer than reasonably necessary for verification and any associated compliance or evidentiary requirement.

B.12 Legal, Regulatory and Dispute Records

Where personal data is relevant to a legal obligation, regulatory matter, investigation, complaint, dispute, claim, litigation, enforcement action, or other formal proceeding, LSR may retain the relevant information for the period necessary to address the matter and any related legal or regulatory requirements.

This may result in information being retained beyond the period that would ordinarily apply to the relevant category of data.

Where a legal hold, regulatory instruction, court order, authority request, investigation requirement, or similar preservation obligation applies, routine deletion or destruction may be suspended for the relevant records.

Once the applicable preservation requirement ends, the records may return to the ordinary retention process unless another lawful basis for continued retention exists.

B.13 Backups, Archives and Deleted Data

Deletion of personal data from active systems may not always result in immediate removal of every copy from backup, disaster recovery, archive, or other protected systems.

Residual copies may remain for a limited period in accordance with backup cycles, disaster recovery procedures, system architecture, security requirements, and applicable retention obligations.

Data retained in backups should not ordinarily be restored or used for routine operational purposes after deletion from active systems except where necessary for disaster recovery, system restoration, security, legal compliance, or another legitimate purpose.

Where a backup containing previously deleted information is restored, LSR may take reasonable measures to ensure that applicable deletion or restriction requirements are reapplied where appropriate.

Historical archives that constitute independent legal, regulatory, classification, certification, audit, or evidentiary records may be subject to their own retention requirements and are not treated merely as backup copies.

B.14 Deletion, Anonymization and Review

At the end of the applicable retention period or when information is no longer reasonably necessary, LSR may review the relevant records to determine the appropriate action.

Depending on the nature of the information and applicable requirements, LSR may:

- Securely delete or destroy the information;
- Anonymize the information;
- Remove or redact unnecessary personal data from a record;
- Restrict further processing;
- Transfer information to an appropriate historical archive;
- Retain specific information where a continuing lawful retention requirement exists.

Anonymized information that can no longer reasonably be associated with an identifiable individual may be retained and used for statistical, analytical, operational, historical, research, quality, or service-improvement purposes, subject to applicable law.

LSR may periodically review retention practices and update applicable retention schedules as its services, systems, legal obligations, regulatory requirements, and professional activities develop.

Appendix C — Categories of Recipients

This Appendix provides an overview of the principal categories of persons, organizations, authorities, and service providers that may receive or access personal data processed by LSR.

The categories described below are illustrative and do not mean that personal data is routinely shared with every category of recipient.

The actual recipient, scope of disclosure, and categories of personal data involved will depend on the relevant service, processing purpose, authorization, legal basis, regulatory requirement, contractual relationship, and operational circumstances.

Where reasonably practicable, LSR will limit access or disclosure to personal data that is relevant and necessary for the applicable purpose.

Where a recipient processes personal data on behalf of LSR, appropriate contractual, confidentiality, security, and data protection requirements may apply. Where a recipient acts independently under its own legal authority or responsibilities, that recipient may be independently responsible for its processing of personal data.

C.1 Categories of Recipients

Category of Recipient	Examples	Typical Purposes of Disclosure or Access	Personal Data That May Be Involved	General Safeguards / Conditions
Flag Administrations and Maritime Administrations	Flag States, maritime administrations, delegated maritime authorities	Statutory certification, authorization, survey oversight, certificate verification, regulatory reporting, vessel status, investigations, compliance	Identity, contact, professional, vessel-related, survey, audit, certification, authorization and document data	Disclosure limited to relevant official functions and subject to applicable law, authorization arrangements and regulatory requirements
Port State and Other Competent Authorities	Port State Control authorities, maritime authorities, government bodies, regulators, courts, law	Inspections, investigations, certificate verification, enforcement, casualty or safety matters, compliance, legal obligations	Identity, professional, certification, vessel, communication, security, audit and documentary records	Legal authority and scope of request may be assessed; disclosure limited where reasonably practicable to information

Category of Recipient	Examples	Typical Purposes of Disclosure or Access	Personal Data That May Be Involved	General Safeguards / Conditions
	enforcement authorities			necessary for the lawful purpose
Recognized Organizations and Classification Societies	Recognized Organizations, classification societies, technical organizations	Transfer of class, statutory services, verification, technical cooperation, continuity of records, regulatory compliance	Vessel history, survey records, certification information, professional identities, approvals, technical submissions and correspondence	Subject to applicable professional requirements, agreements, confidentiality obligations and data protection requirements
Surveyors, Auditors, Inspectors and Technical Personnel	Authorized surveyors, auditors, inspectors, technical reviewers, engineers	Survey, audit, inspection, technical review, verification, certification and corrective action activities	Identity, professional, vessel, document, certification, application, communication and technical information	Role-based and assignment-based access; confidentiality, professional, contractual and security obligations may apply
Authorized LSR Personnel	Administrators, reviewers, approvers, technical personnel, support personnel, management	Portal administration, service delivery, review, approval, security, support, compliance and operational management	Relevant account, identity, professional, application, vessel, document, communication, security and audit information	Access restricted according to role, responsibility, operational necessity and authorization
Vessel Owners, Managers and Operators	Registered owners, ship managers, operators	Vessel administration, service requests, classification, certification, surveys, audits, documentation	Professional identities, contact details, vessel records, applications, certificates, reports, workflow	Access determined by organizational relationship, user role, permissions and

Category of Recipient	Examples	Typical Purposes of Disclosure or Access	Personal Data That May Be Involved	General Safeguards / Conditions
		and communication	and communication data	relevant service authorization
DOC Holders and Safety Management Organizations	ISM Company / DOC holder	ISM-related audits, certification, company-vessel relationships, compliance, document review	Professional, organizational, audit, certification, vessel, communication and supporting document data	Access limited to the relevant relationship, responsibility and applicable service
Charterers, Agents and Authorized Representatives	Bareboat charterers, vessel agents, legal or operational representatives	Service coordination, applications, documentation, vessel representation, operational communications	Identity, contact, professional, authority, vessel, request and document data	Appropriate authority or relationship should exist; access does not authorize unrelated use or further disclosure
Applicants and Client Organizations	Companies applying for LSR services, authorized client entities	Applications, onboarding, service management, verification and operational workflows	Identity, contact, professional, company, application, document and workflow information	Access and disclosure based on the relevant application, organization, authorization and Portal permissions
Technology and Infrastructure Providers	Hosting providers, cloud or server services, software providers, infrastructure vendors	Hosting, storage, backup, system operation, maintenance and technical infrastructure	Account, technical, usage, document, communication or other data required for the service	Contractual restrictions, confidentiality, security obligations, processing instructions and international transfer

Category of Recipient	Examples	Typical Purposes of Disclosure or Access	Personal Data That May Be Involved	General Safeguards / Conditions
				safeguards where applicable
Communication Service Providers	Email delivery services, messaging infrastructure, notification providers	Verification emails, notifications, security alerts, service correspondence	Name, email address, message metadata and message content where necessary	Processing limited to communication services and subject to appropriate contractual and security requirements
Authentication and Verification Providers	Identity verification, authentication or security providers	Identity verification, account security, authentication, fraud prevention	Identity, account, authentication, device and technical information	Data minimization, security, contractual restrictions and applicable verification requirements
Cybersecurity and Security Service Providers	Security monitoring, incident response, threat detection providers	Security monitoring, fraud prevention, vulnerability management, incident investigation	IP addresses, account identifiers, authentication records, logs, device information, security events	Access limited to security purposes and protected by appropriate confidentiality, technical and contractual controls
Analytics and Performance Providers	Analytics, monitoring or performance services where used	Portal performance, error detection, usage analysis and service improvement	Technical, device, usage, session and performance information	Consent where required; minimization, aggregation, de-identification or anonymization where appropriate

Category of Recipient	Examples	Typical Purposes of Disclosure or Access	Personal Data That May Be Involved	General Safeguards / Conditions
External Databases and Verification Sources	Official vessel registers, company registers, professional registers, regulatory databases	Verification, compliance, professional checks, vessel information validation	Identity, professional, company, vessel and authorization information	Information accessed or exchanged only where relevant and legally permitted
Professional Advisers	Lawyers, accountants, auditors, compliance advisers, consultants, experts	Legal advice, compliance, audit, governance, contractual matters, risk management, investigations	Personal data relevant to the professional matter concerned	Professional confidentiality, contractual confidentiality, legal privilege or other applicable protections
Insurers and Insurance-Related Parties	Insurers, brokers, claims professionals	Insurance matters, claims, risk assessment, incidents, legal disputes	Identity, professional, vessel, incident, survey, audit, communication and documentary information	Disclosure limited to relevant insurance or claims purpose and applicable legal or contractual requirements
Courts and Dispute Resolution Bodies	Courts, tribunals, arbitrators, mediators	Legal proceedings, claims, disputes, enforcement and defence of legal rights	Any personal data relevant and lawfully necessary to the proceeding	Disclosure subject to applicable legal process, procedural requirements and relevance
Corporate Transaction Parties	Prospective buyers, successors, investors,	Merger, acquisition, restructuring, transfer of business or	Personal data relevant to the business or	Confidentiality and due diligence controls; further safeguards or notice where

Category of Recipient	Examples	Typical Purposes of Disclosure or Access	Personal Data That May Be Involved	General Safeguards / Conditions
	transaction advisers	assets, succession	operations involved	required by applicable law
Emergency and Safety-Related Recipients	Emergency authorities, rescue organizations, competent safety bodies	Protection of life, health, vessel safety, casualty response or urgent maritime situations	Identity, contact, vessel, professional, emergency and relevant safety information	Disclosure limited to what is necessary for the emergency or lawful safety purpose
Other Recipients Required or Permitted by Law	Other legally authorized public or private bodies	Compliance with legal obligations or another lawful and legitimate purpose	Personal data relevant to the particular lawful requirement	Disclosure only where an appropriate legal basis, obligation, authority or other lawful justification exists

C.2 Recipient Access and Disclosure Principles

LSR will seek to apply the following principles when personal data is disclosed to or accessed by recipients:

- access and disclosure should have an identifiable and legitimate purpose;
- the recipient should receive only information reasonably necessary for that purpose;
- access should be limited according to authorization, role, responsibility, and operational necessity where applicable;
- recipients processing personal data on behalf of LSR may be subject to contractual processing instructions and confidentiality, security, retention, and data protection obligations;
- international disclosures or access may be subject to the safeguards described in Section 9 and Appendix D of this Privacy Policy;
- disclosure to competent authorities may be made where required or permitted by applicable law;
- receiving personal data does not authorize a recipient to use the information for unrelated purposes;

- LSR may maintain records of disclosures or access where necessary for accountability, audit, security, compliance, or legal purposes.

The identification of a category of recipient in this Appendix does not mean that every recipient within that category is authorized to receive all categories of personal data.

C.3 Independent Controllers and Processors

The legal role of a recipient may vary depending on the relevant processing activity.

A recipient may act as:

- a **processor or service provider**, processing personal data on behalf of LSR and according to applicable instructions;
- an **independent controller**, determining its own purposes and means of processing under its legal, regulatory, contractual, or professional responsibilities;
- a **joint or otherwise shared participant** in a processing activity where responsibilities are determined according to applicable law and the relevant arrangement.

For example, a technology provider hosting information on behalf of LSR may act as a processor for the relevant service, while a flag administration receiving information in the exercise of its statutory authority may process that information independently under its own legal responsibilities.

The classification of a recipient depends on the actual circumstances of the processing and will not be determined solely by the category in which the recipient is listed in this Appendix.

C.4 Changes to Recipient Categories

The categories of recipients used by LSR may change as LSR services, technologies, regulatory responsibilities, operational arrangements, and professional relationships develop.

The appointment of a new service provider or the introduction of a new category of recipient will not automatically authorize disclosure of personal data. The relevant processing purpose, legal basis, necessity, contractual requirements, security measures, international transfer requirements, and other applicable data protection obligations must be considered.

Where a change to recipients materially affects the processing of personal data and applicable law requires notice, consent, or another action, LSR will take the required measures

Appendix D — International Data Transfer Framework

This Appendix describes the general framework LSR may apply when personal data is transferred, accessed, disclosed, stored, or otherwise processed across national borders.

Because maritime activities are inherently international, personal data may need to move between countries in connection with vessel operations, classification, statutory certification, surveys, audits, technical reviews, regulatory oversight, service providers, professional advisers, and other activities described in this Privacy Policy.

International transfers will be assessed according to the applicable legal framework, the purpose and necessity of the transfer, the nature of the personal data involved, the recipient, the destination country, the role of the recipient, and the safeguards available for the relevant processing activity.

The framework described in this Appendix does not create an obligation to transfer personal data where the transfer would be prohibited or otherwise unlawful under applicable data protection law.

D.1 International Transfer Scenarios

International transfers may arise in circumstances including:

- classification and statutory certification activities;
- vessel surveys, audits, inspections, and technical reviews;
- communication with flag administrations and maritime authorities;
- transfer of class or certification responsibility;
- use of surveyors, auditors, inspectors, consultants, or technical personnel located in another jurisdiction;
- use of hosting, infrastructure, communication, cybersecurity, verification, analytics, or other technology providers;
- legal, regulatory, compliance, insurance, audit, or professional advisory matters;
- investigations, casualties, incidents, claims, or disputes;
- corporate transactions or organizational changes;
- other situations where cross-border processing is reasonably necessary for a lawful LSR activity.

The fact that a service or recipient is located outside the country in which personal data was collected does not, by itself, determine whether a transfer is lawful. The applicable transfer conditions will depend on the relevant legal framework and circumstances.

D.2 Assessment of Transfer Requirements

Before or in connection with an international transfer, LSR may consider factors including:

- the country or jurisdiction from which the personal data originates;
- the destination country or jurisdiction;
- the applicable data protection law;
- the purpose and necessity of the transfer;
- the categories and sensitivity of the personal data;
- the identity and legal role of the recipient;
- whether the recipient acts on behalf of LSR or independently;
- applicable legal, regulatory, statutory, contractual, or professional requirements;
- the safeguards available for the transfer;
- technical and organizational measures applied to the information;
- the duration and frequency of the transfer;
- whether onward transfers may occur.

Where required by applicable law, LSR may document the relevant assessment and the transfer mechanism relied upon.

D.3 Adequacy and Recognized Transfer Mechanisms

Where applicable data protection law recognizes that a destination country, territory, sector, organization, or legal framework provides an adequate level of protection, LSR may rely on that recognition where the conditions for the relevant transfer are satisfied.

Where no such recognition applies, LSR may rely on another legally recognized transfer mechanism where appropriate.

Such mechanisms may include:

standard contractual clauses or equivalent contractual safeguards;

binding or approved contractual arrangements;

authorized data transfer agreements;

recognized certification or compliance mechanisms;
legally recognized codes, frameworks, or arrangements;
other safeguards expressly permitted under applicable law.

The particular mechanism used will depend on the relevant jurisdiction and circumstances of the transfer.

D.4 Transfers to Flag Administrations and Maritime Authorities

Personal data may be transferred internationally to flag administrations, maritime administrations, port state authorities, recognized organizations, regulatory bodies, or other competent maritime authorities where necessary or permitted in connection with official maritime functions.

Such transfers may relate to:

- statutory certification;
- authorization and delegation arrangements;
- vessel surveys and audits;
- certificate verification;
- regulatory reporting;
- vessel status;
- transfer of class;
- deficiencies, detentions, incidents, or casualty matters;
- investigations;
- compliance with maritime conventions, laws, codes, or administrative requirements.

Where the recipient exercises independent statutory, regulatory, or public authority, the recipient may process personal data under its own legal responsibilities.

LSR will determine the appropriate transfer basis according to the applicable law and the nature of the relevant official function.

D.5 Transfers to Service Providers

LSR may use service providers located in or operating from jurisdictions different from the jurisdiction in which personal data was originally collected.

Such providers may include:

- hosting and infrastructure providers;
- storage and backup providers;

- communication and email services;
- authentication and verification providers;
- cybersecurity providers;
- analytics or performance providers;
- software and technical support providers;
- other operational or technology service providers.

Where a service provider processes personal data on behalf of LSR, LSR may require contractual provisions addressing:

- processing instructions;
- confidentiality;
- security;
- international transfers;
- sub-processors;
- access controls;
- incident notification;
- data retention;
- deletion or return of data;
- cooperation with applicable data protection obligations.

Where required, additional transfer safeguards may be implemented depending on the destination, service, and nature of the personal data.

D.6 Technical and Organisational Safeguards

International transfers may be supported by technical and organizational measures appropriate to the nature and risk of the processing.

Such measures may include:

- encryption in transit or at rest where appropriate;
- secure communication methods;
- restricted and role-based access;
- authentication controls;
- logging and audit trails;
- data minimization;

- segregation of information;
- access approval procedures;
- confidentiality obligations;
- incident response procedures;
- retention and deletion controls;
- other measures intended to reduce unauthorized access, use, disclosure, or loss.

The use of a technical safeguard does not replace a legal transfer mechanism where applicable law requires one.

D.7 Transfer Minimisation

Where reasonably practicable, LSR will seek to limit international transfers to personal data relevant and necessary for the applicable purpose.

This may include:

- transferring only required fields or records;
- limiting recipient access to the relevant vessel, company, request, certificate, or workflow;
- using anonymized, aggregated, redacted, or de-identified information where identifiable personal data is not required;
- avoiding transfer of unnecessary sensitive information;
- applying time-limited or role-limited access where appropriate.

Transfer minimisation does not require LSR to remove information where the complete record is necessary for legal, regulatory, classification, certification, technical, audit, evidentiary, or other legitimate purposes.

D.8 Onward Transfers

A recipient located in another jurisdiction may, in some circumstances, need to transfer personal data onward to another recipient or jurisdiction.

Where a recipient processes personal data on behalf of LSR, onward transfers may be subject to contractual restrictions, authorization requirements, security obligations, and applicable transfer safeguards.

Service providers may be required to obtain appropriate authorization before appointing sub-processors or transferring personal data to additional locations, where required by the relevant contractual or legal framework.

Where a recipient acts independently under its own statutory, regulatory, legal, or professional responsibilities, any onward processing may be governed by the legal obligations applicable to that recipient.

D.9 Exceptional and Necessary Transfers

Applicable data protection law may permit international transfers in specific circumstances even where another transfer mechanism is not available.

Depending on the relevant law, such circumstances may include transfers necessary for:

- performance of a contract or steps requested by the individual;
- conclusion or performance of certain arrangements made in the interest of the individual;
- important reasons of public interest;
- establishment, exercise, or defence of legal claims;
- protection of vital interests;
- lawful access to certain public registers;
- other exceptions or derogations expressly recognized by applicable law.

LSR will rely on such an exception only where the relevant legal conditions are satisfied and where its use is appropriate to the circumstances.

D.10 International Access to Portal Data

An international transfer may occur not only when information is physically sent from one country to another, but also where personal data stored in one jurisdiction is remotely accessed from another jurisdiction, to the extent such access constitutes an international transfer under applicable law.

Accordingly, access by authorized surveyors, auditors, personnel, service providers, administrators, or other recipients located in another jurisdiction may be subject to the same transfer assessment and safeguards applicable to other cross-border processing.

LSR may use role-based permissions, assignment controls, technical restrictions, logging, and other measures to limit remote access according to legitimate operational requirements.

D.11 Transfer Records and Governance

Where appropriate or required by applicable law, LSR may maintain records concerning international transfers.

Such records may include:

- categories of personal data transferred;
- categories or identity of recipients;
- destination jurisdictions;
- transfer purposes;
- applicable legal basis or transfer mechanism;

- safeguards used;
- service provider or contractual arrangements;
- transfer assessments;
- relevant security measures;
- review or approval information.

LSR may periodically review international transfer arrangements where necessary due to changes in law, service providers, destination jurisdictions, processing activities, technology, regulatory requirements, or identified risks.

D.12 Individual Rights in Relation to International Transfers

Where provided by applicable law, individuals may request information regarding international transfers involving their personal data, including the categories of recipients, destination jurisdictions, or safeguards used for relevant transfers.

The scope of information that can be provided may be subject to legal, contractual, confidentiality, security, or other lawful restrictions.

Requests relating to international transfers may be submitted through the privacy contact mechanisms described in this Privacy Policy.

The existence of an international transfer does not remove or reduce any data protection rights that apply to the processing under applicable law.

Appendix E — Privacy Policy Version History

Version	Effective Date	Revision Type	Summary of Changes	Approved By
1.0.0	26.07.2026	Initial Release	Initial publication of the LSR Privacy Policy, including provisions concerning personal data collection, processing purposes, legal bases, data sharing, international transfers, retention, security, cookies and local storage, automated processing and artificial intelligence, individual rights, third-party services, children’s privacy, policy updates, and related appendices.	Life At Sea Register