Vendor Privacy Notice

Lloyds Offshore Global Services Private Limited (operating as Lloyds Technology Centre – ("Company"))

1. Who this notice applies to

This privacy notice applies to vendors, suppliers, consultants, sole proprietors, and individuals acting on behalf of vendor organizations who interact with the Company in the context of a commercial or contractual relationship ("Vendors").

Personal data shared by vendors is voluntary and collected where necessary for vendor onboarding, due diligence, contract management, payment processing, compliance, security, and ongoing relationship management. Such personal data is accessed only by authorised personnel on a need-to-know basis and stored within Company-approved systems and repositories in accordance with applicable retention, security and governance requirements.

2. What this notice covers

- Vendor onboarding and due diligence activities
- Contract negotiation, execution, and administration
- Business communications and relationship management
- Invoice processing and payments
- Regulatory, audit, and compliance activities
- Information security and access management (vendor contact level)

This notice does not cover background verification of vendor personnel, investigations, or processing carried out by vendors on behalf of the Company as processors. Where applicable, these activities are governed by valid contractual arrangements.

3. Information we collect from Vendors

Much of the information we collect in the vendor onboarding and relationship process relates to the vendor organization (i.e., company information). Where we collect details relating to an identifiable individual (for example, a vendor's authorized representative or point of contact), those details are treated as personal data.

- Vendor organization information (e.g., legal entity name, registered address, registration/incorporation details, GSTIN (if applicable), nature of services)
- Vendor contact / representative details (personal data) (e.g., name, job title, business email address, business phone number)
- Due diligence and compliance information about the vendor organization (e.g., corporate documentation provided during onboarding, sanctions/financial crime screening results at entity level, risk assessments)

- Payment and invoicing information (primarily vendor/company information) (e.g., bank account details for payments, invoice details, payment references, tax-related information)
- Records of business communications and contractual interactions (e.g., emails, meeting notes, contract correspondence, support tickets). These records may include vendor contact / representative details.

We do not intentionally collect personal data beyond what is necessary to manage the vendor relationship. Access to such personal data is restricted to authorised personnel on a need-to-know basis and limited to the minimum personal data necessary for the relevant business, including for legal, regulatory, audit or compliance purposes.

Where personal data is included within vendor documentation or communications, it will be handled in accordance with applicable law and internal controls.

4. Why we use your personal data

- To onboard and manage vendor relationships
- To enter into, perform, and manage contracts
- To process invoices and make payments
- To communicate regarding services, deliverables, and obligations
- To meet legal, regulatory, audit, and governance requirements
- Managing information security, risk, and access controls

5. Lawful basis for processing

- For performance of our contracts and management of the vendor relationship
- For certain legitimate uses under applicable law (for example, where processing is reasonably expected in the context of a commercial relationship).
- To comply with applicable laws, regulatory requirements, and lawful requests

We do not rely on consent for routine vendor personal data processing unless specifically required by law or for a specific optional activity. Where we do rely on consent, you may withdraw your consent at any time using the method communicated at the time consent was obtained.

6. Who do we share your personal data with

Access to personal data is restricted to authorised personnel on a need-to-know basis such as to:

- Internal procurement, finance, audit, legal, IT, security, and business teams
- Third-party service providers supporting procurement, payment, or IT systems
- Group entities or regulators, where required by law or contract

All recipients are required to process personal data securely and only for authorized purposes.

7. How long do we keep your personal data

We retain vendor personal data only for as long as necessary for the purposes described in this notice and thereafter delete or anonymize such personal data once the purpose is no longer served, unless retention is required under applicable law. Retention periods are determined based on factors such as (i) the duration of the contractual/commercial relationship, (ii) applicable limitation periods, and (iii) legal, regulatory, audit, and records-management obligations (including requirements to maintain procurement and financial records). Data is then securely deleted or anonymized in accordance with the Company records management procedure.

8. International transfers

In some cases, vendor personal data may be processed or accessed by authorized teams or service providers located outside India (for example, where group functions or technology platforms are operated from other locations). Where this occurs, we implement appropriate contractual and organizational safeguards and ensure that such transfers are permitted under applicable law (including any restrictions notified under the Digital Personal Data Protection Act, 2023).

9. Security Practices

The Company implements appropriate managerial, technical, operational and physical controls, consistent with applicable data protection laws and Group standards, to safeguard personal data against unauthorized or unlawful access, loss, misuse, alteration or disclosure and to meet reasonable security safeguards requirements under applicable law.

10. Your Rights

a) Right to access information about personal data: You have the right to access information about the personal data processed by us, including where such personal data is processed on our behalf by a third party.

b) Right to correction and erasure of personal data: You have the right to request correction, completion, updating, and erasure of your personal data processed by us, including where such personal data is processed on our behalf by a third party.

c) Right to nominate: You have the right to nominate any individual who may exercise your rights in the event of death or incapacity (inability to exercise the rights due to unsoundness of mind or infirmity of body).

d) Right to withdraw consent: If we process your personal data based on your consent, you can withdraw that consent at any time.

e) Right to grievance redressal: You can raise grievance with us if you believe we have not met our obligations under the DPDPA or if you are not able to exercise your rights.

f) Right to approach the Data Protection Board of India: Where you have raised a grievance with us and it has not been resolved within the timelines prescribed under applicable law, you may have the right to escalate the matter to the Data Protection Board of India, in accordance with the Digital Personal Data Protection Act and applicable rules.

Details on how to exercise these rights, including contact details for the Data Protection Officer and Grievance Officer, are provided in the Lloyds Technology Centre Website Privacy Notice available at https://lloydstechnologycentre.com/privacy-policy

11. Updates to this notice

This Privacy Notice may be updated from time to time to reflect changes in law, regulation, or business practices. The latest version will always be made available through appropriate channels.