DATA PROTECTION AND INFORMATION SECURITY STATEMENT

S.No	Revision	Date	Prepared By	Approved By
1	0	20 May 2026	Kosal Ram N	Sanjai PT

DATA PROTECTION AND INFORMATION SECURITY STATEMENT

IAN PROCUREMENT SOLUTIONS

(For International Clients — Europe, United Kingdom, United States & Middle East)

---

1. INTRODUCTION

IAN Procurement Solutions (“IAN”) is committed to protecting the confidentiality, integrity, and lawful processing of personal data and client confidential information entrusted to us.

As a procurement and supply chain support service provider working with organisations in the European Union and the Middle East, including the State of Qatar and the United Arab Emirates (Dubai), IAN maintains structured internal policies aligned with:

- **EU General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)**
- **UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018**
- **Applicable United States state privacy laws (e.g., California Consumer Privacy Act / CPRA), where personal data of US residents is processed**
- **Qatar Personal Data Privacy Protection Law No. 13 of 2016**
- **UAE Federal Decree Law No. 45 of 2021 on the Protection of Personal Data (PDPL)**

IAN acts as a Data Processor for services involving personal data and processes data strictly in accordance with documented client instructions.

---

2. ROLE IN DATA PROCESSING

Where personal data is involved:

- The Client remains the **Data Controller** and determines the purpose and means of processing.
- IAN acts solely as the **Data Processor**, processing data only as instructed in writing.

IAN does not independently determine purposes of processing unless specifically agreed in a separate contractual arrangement.

A formal Data Processing Agreement (DPA) is executed before commencement of services involving personal data. For EU and UK clients, this DPA incorporates the EU Standard Contractual Clauses (Module 2: Controller-to-Processor) and, where applicable, the UK International Data Transfer Addendum (IDTA), in addition to Article 28 GDPR processor obligations.

IAN has designated Mr. Kosal Ram N – Chief Compliance Officer, as its Data Protection Officer / Privacy Lead, contactable at info@iantechnologies.com, responsible for oversight of this framework and for liaising with Controllers on data protection matters.

---

3. LAWFUL PROCESSING PRINCIPLES

IAN processes personal data in accordance with the following principles:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality

Processing activities are limited strictly to procurement support, vendor coordination, contract documentation, and supply chain management functions defined in the service agreement.

---

4. ACCESS CONTROL FRAMEWORK

IAN maintains a formal **Access Control Policy** designed to prevent unauthorised access to client data.

Controls include:

- Role-based access rights (least privilege principle)
- Unique user identification for each authorised individual
- Immediate access revocation upon termination or role change
- Periodic access review
- Restricted access to sensitive commercial and personal data

Access to client data is granted only where operationally necessary.

---

5. PASSWORD AND AUTHENTICATION SECURITY

IAN enforces a structured **Password and Authentication Policy** applicable to:

- Laptops and desktops
- Email systems
- ERP and procurement platforms
- Cloud storage solutions
- Network-connected devices

Security controls include:

- Strong password requirements
- Periodic password rotation

- Multi-factor authentication where available
- Prohibition of shared credentials
- Automatic screen locking
- Secure remote access protocols

---

6. CROSS-BORDER DATA TRANSFER

Where personal data originating from the EU, Qatar, or UAE is processed in India:

- Processing is conducted under contractual safeguards defined in the Data Processing Agreement, including the EU Standard Contractual Clauses (SCCs) and/or UK International Data Transfer Addendum (IDTA) where personal data originates from the EU or UK, given that India does not currently hold an EU/UK adequacy decision. y.
- Data is processed solely for the purpose authorised by the Controller.

IAN does not transfer personal data to third parties without written authorisation from the Controller.

---

7. DATA SUBJECT RIGHTS SUPPORT

Where required under GDPR, Qatar PDPL, or UAE PDPL, IAN:

- Assists the Controller in responding to data subject access requests
- Supports correction, deletion, or restriction of processing upon instruction
- Cooperates in regulatory inquiries where legally required

IAN does not respond directly to data subjects unless instructed by the Controller.

---

8. INCIDENT MANAGEMENT AND BREACH RESPONSE

IAN maintains a formal **Incident Reporting and Response Procedure**.

In the event of a suspected or confirmed personal data breach:

- - Immediate containment actions are initiated

- Internal assessment is conducted

- The Client is notified within 24 hours of IAN confirming a personal data breach, to support the Controller's own regulatory notification obligations (e.g., the 72-hour requirement under GDPR Article 33)

- Corrective measures are implemented

- All incidents, whether or not reportable to a regulator, are logged in an internal breach register in line with GDPR Article 33(5)

9. CONFIDENTIALITY AND EMPLOYEE OBLIGATIONS

All employees and contractors:

- Sign confidentiality undertakings
- Receive internal policy awareness
- Are bound to handle client data strictly within authorised scope

Unauthorised disclosure or misuse of client data results in disciplinary action.

---

10. DATA RETENTION

IAN retains personal data only for the duration necessary to fulfil contractual obligations, and in any event for no longer than the term of the service agreement plus 24 months, unless the Controller instructs earlier deletion or a longer period is required by applicable law.

Upon termination of services, personal data is returned to the Controller or securely deleted within 30 days, in accordance with client instructions and contractual terms.

---

11. CONTINUOUS COMPLIANCE AND REVIEW

IAN periodically reviews its data protection controls to ensure alignment with:

- GDPR requirements
- United States state privacy laws
- Qatar PDPL requirements
- UAE PDPL requirements
- Contractual obligations with international clients

Security and governance controls are updated as necessary to reflect regulatory or operational developments.

---

12. CLIENT ASSURANCE

IAN Procurement Solutions operates as a structured, compliance-oriented service provider with formal policies governing:

- Access Control
- Password and Authentication Security
- Data Processing Agreements
- Incident Reporting and Breach Response

- Confidentiality and Conflict of Interest

We are committed to maintaining professional, ethical, and legally compliant standards in all engagements with European and Middle East clients.

For further information regarding our data protection framework, please contact:

Data Protection Officer / Privacy Lead: Mr. Kosal Ram N

Email: info@iantechnologies.com

End of Data Protection and Information Security Statement