PRIVACY NOTICE FOR CLIENTS AND SUPPLIERS
Pursuant to Art. 13–14 2016/679 (EU) Regulation ("GDPR")

This privacy notice describes the processing of personal data carried out by the companies of the TÜV Rheinland Group in Italy, in its capacity as Data Controller, in the context of contractual relationships with its clients, business partners, suppliers and the supply chain.

1. Who is the Data Controller? How can it be contacted?

The "Data Controller" is, alternatively, the TÜV Rheinland Group company in Italy acting as contractual counterparty in the relevant relationship, as expressly identified in the Offer, in the Contract and/or in the General Terms and Conditions.
In particular, the "Controller" may be one of the following companies:

- **TÜV Rheinland Italia S.r.l.** a socio unico, registered office at Via Enrico Mattei 3, 20005 Pogliano Milanese (MI), Italy, Tax Code and VAT No. 12184570153;
- **ICARO S.r.l.** a socio unico, registered office at Piazza Duomo 1, 52044 Cortona (AR), Italy, Tax Code and VAT No. 01155020512;
- **HON Consulting S.r.l.** a socio unico, registered office at Via Lepanto 23, 59100 Prato (PO), Italy, VAT No. 02203700972.

Each company acts as an independent Data Controller with respect to processing activities related to contractual relationships falling within its competence.

For any matter related to the processing of your personal data, you may contact the relevant Data Controller by email at: for TÜV Rheinland Italia S.r.l.: dpr@it.tuv.com; for ICARO S.r.l.: privacy@icarocortona.it; for HON Consulting S.r.l.: h-on.privacy@tuv.com, or by written communication addressed to the postal address indicated above.

2. Who are the Data Subjects?

"**Data Subjects**" are all natural people whose personal data are processed by the Data Controller in connection with the qualification, negotiation, execution, monitoring, and management of contractual relationships, and in particular:

A) In relationships with Clients and business counterparties:

- individual Clients (e.g., professionals, consultants, sole proprietorships);
- employees, collaborators, technicians, and contacts of corporate Clients;
- legal representatives, authorized agents, and administrative/commercial contacts of the Client;
- any other individual designated by the Client as a contractual or operational contact.

B) In dealings with suppliers:

- suppliers who are individuals (e.g., professionals, consultants, sole proprietorships);
- employees, contractors, technicians, and contact persons of suppliers that are legal entities;
- legal representatives, authorized agents, and administrative/commercial contact persons of the Supplier;
- Supplier personnel whose data appear in documentation regarding compliance with social security, insurance, tax, and labor obligations (e.g., F24 tax forms);
- any other natural person designated by the Supplier as a contractual or operational contact.

3. What personal data do we collect and process?

The Data Controller processes only the personal data necessary for the selection, qualification, management, monitoring, and fulfillment of the contractual and commercial relationship.

Categories of data common to both areas:

- identification and personal information (first name, last name, role/title; where a mandatory legal, regulatory, H&S or security check so requires, identity is verified by exhibition of an identification document, recording only its type and number, without acquiring or retaining any copy);
- professional contact information (email, phone number, work address);
- administrative, tax, and banking information of the contracting party (e.g., tax ID number/VAT number, bank account information necessary for payments);
- corporate data relating to the contractual counterparty that is a legal entity (company name, registered office, and operational locations);
- operational information related to orders, deliveries, technical activities, audits, verifications, and interactions with the Data Controller;
- additional personal data strictly necessary and relevant to the negotiation, execution, performance, or termination of the contractual relationship.

Additional categories of data processed solely in relations with Suppliers:

- data regarding compliance with social security, insurance, and tax obligations, as well as labor obligations (e.g., Company Register registration, F24 forms relating to withholding taxes), to the extent necessary to comply with legal requirements and to manage joint and several liability;
- data related to occupational health and safety, limited to the management and reporting of accidents or incidents involving the Supplier's personnel at the Data Controller's premises or during the performance of activities;
- data necessary for sustainability assessments and supply chain due diligence (including declarations and questionnaires regarding human rights, labor, the environment, sanctions, and export controls).

Your personal data will be processed in accordance with the principles of minimization, proportionality and necessity, processing only the necessary data and using manual, computerized, and telematic tools equipped with security measures suitable for ensuring the confidentiality and integrity of the data.

4. Where do personal data come from?

Personal data is generally provided by employees and/or appointed and authorized representatives of the Data Controller's contractual counterparty, or by the contractual counterparty itself, which discloses such data to the Data Controller. Additional data may be generated automatically during the use of the Group's IT platforms.
In dealings with suppliers only, additional data may come from compliance and employment documentation submitted by the Supplier and from public databases and registries (e.g., the Company Register).

5. For what purposes do we process data? What is the legal basis? How long are they retained?

Purpose	Applies to	Legal Basis	Retention period
1. Management of contractual and pre-contractual relationships: assessment, classification, negotiation, execution, and performance of contractual relationships, including the management of orders, deliveries, supplies, services, contractual audits, and operational communications.	Clients and Suppliers	Art. 6(1)(b) GDPR, when the data subject is a party to the contract, such as a natural person or sole proprietorship acting as the other party. Art. 6(1)(f) GDPR, for the processing of data pertaining to contacts, employees, collaborators, and representatives of the client or supplier company, based on the Data Controller's legitimate interest in managing and executing the contractual relationship.	For the entire duration of the relationship and for 10 years following its termination, corresponding to the ordinary limitation period under Article 2946 of the Italian Civil Code. Where the same data are also processed for one of the purposes below carrying a longer statutory period, that longer period prevails for those data only.
2. Administrative, accounting, and tax compliance: management of administrative, accounting, and tax compliance obligations, including bookkeeping, invoicing, and reporting to the relevant authorities and regulatory or supervisory bodies.	Clients and Suppliers	Art. 6(1)(c) of the GDPR - compliance with legal obligations.	10 years from the date of the accounting entry or for the different period provided for by applicable law, pursuant to, among other provisions, Article 2220 of the Italian Civil Code, Article 22 of Presidential Decree No. 600/1973, and Article 39 of Presidential Decree No. 633/1972.
3. Compliance, qualification and due diligence activities: processing activities necessary to assess, verify and monitor the reliability, integrity and compliance of counterparties and suppliers, including for the purposes of risk management, audit, health and safety, information security, sustainability, supply chain due diligence, compliance with applicable laws, internal policies, Group standards and contractual requirements, in each case where applicable and to the extent relevant to the specific relationship.	Clients and Suppliers, depending on the nature of the relationship and the specific checks required. Certain checks generally apply only to Suppliers or to counterparties involved in higher-risk activities.	Art. 6(1)(c) GDPR, where the processing is necessary to comply with legal obligations applicable to the Data Controller. Art. 6(1)(f) GDPR, where the processing is based on the Data Controller's legitimate interest in verifying the integrity, reliability, security and compliance of counterparties and of the supply chain, preventing unlawful conduct, protecting the organisation and ensuring compliance with internal policies and group standards. For health-related data, only when it is necessary and limited to the management and reporting of injuries, accidents or safety incidents: Art. 9(2)(b) GDPR, in conjunction with applicable occupational health and safety legislation, including Legislative Decree 81/2008 and the relevant provisions of the Italian Privacy Code. In emergency situations, where strictly necessary, Art. 9(2)(c) GDPR may also apply.	For the duration of the relationship and, thereafter, for the period necessary to comply with applicable legal obligations or to establish, exercise or defend legal claims. As a rule, records are retained for no longer than 10 years, unless a shorter or longer period applies to the specific document category or legal obligation. Health-related data processed for the management and reporting of accidents or safety incidents are retained only for the time necessary to manage the relevant event and related obligations.
4. Establishment, exercise or defence of legal claims: establishing, exercising, or defending the Data Controller's rights in judicial, extrajudicial, administrative, or arbitration proceedings, including litigation, complaints, debt collection, management of defaults, enforcement of guarantees, and related investigative activities.	Clients and Suppliers	Art. 6(1)(f) of the GDPR - the Data Controller's legitimate interest in protecting its rights.	For the entire duration of the litigation or the pre-litigation phase and, subsequently, for the applicable statute of limitations periods - typically 10 years pursuant to Article 2946 of the Italian Civil Code - unless specific time limits apply to the individual case. In the absence of litigation, the data are retained in accordance with the retention periods established for the primary purpose for which they were collected.
5. Extraordinary Group Transactions: management of corporate, extraordinary, or reorganizational transactions, such as mergers, demergers, sales of businesses or business units, acquisitions, contributions of assets, due diligence, intra-group transfers, or other corporate reorganization transactions.	Clients and Suppliers	Art. 6(1)(f) of the GDPR - the Data Controller's legitimate interest in managing corporate transactions and ensuring business continuity, protecting its assets, and properly allocating relationships, contracts, rights, and obligations.	For the time strictly necessary to manage the transaction and, in any case, generally no later than 24 months from the conclusion of the transaction, unless otherwise required by law or necessary for retention for contractual, administrative, accounting, or rights protection purposes.

6. Is the provision of data mandatory?

The provision of data is necessary to establish and manage the contractual relationship. Failure to provide essential data prevents the Data Controller from proceeding with the evaluation, qualification, or execution of the contract.
In dealings with suppliers, for documentation regarding compliance with social security, insurance, and tax obligations, the provision of data is required by law and by the contract: failure to provide such data or the provision of incomplete data may result, in accordance with the General Terms and Conditions of Purchase, in the suspension of payments and/or performance, up to and including the termination of the relationship.

7. Who may receive the data?

The data may be processed or disclosed to:

- authorized personnel of the Data Controller (e.g., those in the Purchasing, Administration, Finance, ICT, HSE, Quality, Compliance, Legal departments);
- companies within the TÜV Rheinland Group, complete list of companies available here, that support the Data Controller in system management, qualification, audit, administrative and/or compliance activities, depending on the case, as independent data controllers or as data processors pursuant to applicable data protection arrangements;
- IT and cloud service providers, subcontractors and consultants appointed as Data Processors pursuant to Article 28 of the GDPR;
- public authorities and regulatory bodies; in dealings with suppliers, in particular, INPS, INAIL, the Italian Revenue Agency, Prefectures, and competent public authorities, accreditation bodies, and sector-specific authorities;
- parties involved in extraordinary Group transactions (e.g., mergers, acquisitions, reorganizations).

8. Are data transferred outside the European Union?

Yes, in some cases. The use of Group-wide shared platforms, such as SAP, and cloud services, may involve transfers to third countries. The Data Controller ensures that such transfers are carried out in compliance with Articles 44–49 of the GDPR, through:

- the European Commission's Standard Contractual Clauses (SCCs),
- Appropriate technical and organizational protection measures;
- Any adequacy decisions by the European Commission, if applicable.

In particular, the Data Controller conducts appropriate assessments regarding the equivalence of the protection offered in the countries to which the data is transferred and adopts the SCCs and supplementary measures required by applicable law. Upon request, the Data Controller may provide information on the safeguards adopted, subject to confidentiality obligations.

9. How long are data retained?

Personal data is retained for the periods specified in the table in Section 5.

Retention periods may be extended where necessary to comply with legal obligations, respond to audits or inspections, or establish, exercise or defend legal claims.

10. What are the Data Subjects' rights?

Data subjects may exercise the rights provided for in Articles 15–22 of the GDPR, specifically:

1. Right of access
2. Right to rectification
3. Right to erasure
4. Right to restriction of processing
5. Right to data portability
6. Right to object
7. Right not to be subject to automated decision-making. However, no automated decision-making, including profiling, is carried out in connection with this privacy notice.

11. How can rights be exercised?

Requests may be sent directly to the Data Controller responsible for the specific contractual relationship using the following contact information:

- for **TÜV Rheinland Italia S.r.l.**: dpr@it.tuv.com
- for **ICARO S.r.l.**: privacy@icarocortona.it
- for **HON Consulting S.r.l.**: h-on.privacy@tuv.com

The Data Controller will respond within 30 days, subject to any extensions permitted by the GDPR.
Finally, we remind you that, in case you consider your rights have been infringed, you have the right to file a complaint with the Italian Data Protection Authority, located in Rome at Piazza Venezia 11, 00187 Rome, Tel. (+39) 06.696771, email: protocollo@gpdp.it, certified email (PEC): protocollo@pec.gpdp.it.

12. Can this Notice be updated?

Yes. This privacy policy may be amended to reflect regulatory, organizational, or technological changes. Updated versions will be made available through the Data Controller's official channels.