1. GENERAL INFORMATION

For the purposes of managing customer/supplier relations in the context of its commercial activities, the UTAC Group collects and processes personal data of commercial contacts from its customers, leads, partners and suppliers.

This notice describes the personal data we collect and the purposes for which they are processed. This notice meets the obligation laid down by Articles 12, 13 and 14 of the GDPR.

2. CATEGORIES OF PERSONAL DATA COLLECTED

The categories of Personal Data we process are:

- Identification of the person concerned (civility, surname, first name);
- Professional life (job title, professional email, professional phone, name of the company of membership);
- Tracking the business relationship:
  - Documentation requests, trial requests, items, product purchased, service or subscription purchased, services ordered and invoiced, quantity, amount, periodicity, date and amount of order and invoice, invoice due date, terms and delivery address, purchase and service history, return of products, origin of sale (seller, representative, partner, affiliate);
  - Orders, invoices, customer correspondence and after-sales service, exchanges and comments of customers and prospects, person(s) in charge of the customer relationship
  - Contract, Mission Order;
- Integrity assessment: scorecard, records and external questionnaire if applicable
- Customer satisfaction.

3. COLLECTION SOURCES

Personal Data is collected directly from our business contacts or indirectly from other UTAC services.

4. LAWUFUL BASIS, PURPOSE AND RETENTION PERIOD

The personal data are collected for the following purposes:

- Management of the business relationship (selection, orders, contracts, deliverables, customer satisfaction, etc.);
- Direct marketing by email.

The lawful basis for the management of the business relationship may be :

- The execution of a contract when the data subject is an individual (BtoC), e.g. a selft-employed contractor;
- The legitimate interests of UTAC :
  - ensure the follow-up of the commercial relationship;
  - promote our products and attract new customers.

The personal data of the business contacts are kept during the business relationship with the client, supplier, partner.

In the case of direct marketing by email, the personal data of commercial contacts is kept until they exercise their right to object.

The personal data of the leads and inactive business contacts are kept during three years after the last contact.

5. DATA RECIPIENTS

5.1. Internal

Only persons authorised to perform their duties or functions have access to your Personal Data within the strict limits of their respective duties and the performance of those duties and functions. This includes persons belonging to the following services:

- Sales;
- Marketing;
- Quality;
- Accounting;
- Purchasing;
- Legal & Compliance;
- The service concerned by the provision of the service or the delivery of the product.

5.2. External

External recipients who receive communication of your Personal Data for the purposes defined above include:

- Where appropriate, the authorities;
- Where appropriate, the service providers which are processing Personal Data of our business contacts on our behalf.

If applicable, any transfer of your Personal Data to a third country is governed by a specific contract.

6. DATA SECURITY

UTAC guarantees the security of your Personal Data. The Group adopted the following technical and organisational security measures:

Categories	Measures
Raise awareness among users	Inform and raise awareness among those accessing the data
	Write an IT charter
	Define a unique identifier for each user
	Adopt a user password policy
Authenticate users	Require user to change password after reset
	Do not store passwords in clear text
	Limit the number of attempts to access an account

Manage Entitlements	Remove outdated access permissions
	Conduct an annual review of entitlements
	Provide a logging system
Trace access and manage incidents	Inform users of the implementation of the logging system
	Protect logging devices and logged information
	Lay down procedures for notifications of personal data breaches
Secure desktops	Provide automatic session locking procedure
	Use regularly updated antivirus programs
	Install a software firewall
	Obtain user approval before performing any actions on the user's computer
Securing Mobile Computing	Providing means for encrypting mobile equipment
	Make regular backups or synchronisations of data
	Limit network flows to what is necessary
	Secure remote access to mobile computing devices via VPN
Protect the internal computer network	Implement WPA2 or WPA2-PSK protocols for Wi-Fi networks
Secure servers	Limit access to administrative tools and interfaces to only authorised individuals.
	Install critical updates immediately.
	Ensure data availability.
	Use TLS and verify its implementation
Secure websites	Verify that no passwords or identifiers are embedded in URLs.
	Check that user input matches what is expected.
	Collect consent for cookies not necessary for the service
	Perform regular backups.
Back up and plan for business continuity	Store backup media in a safe location away from the primary site.
	Provide security means for conveying backups
	Regularly plan and test business continuity
Archive securely	Implement specific access modalities for archived data
	Securely destroy obsolete archives.
Manage data maintenance and destruction	Record maintenance work in a handrail
	Supervise third-party interventions by an organisation official
	Erase data from any hardware before it is disposed of.
Manage outsourcing	Include specific clauses in subcontractors' contracts.
	Lay down the conditions for the return and destruction of data.
	Ensure the effectiveness of the safeguards provided for (security audits, visits, etc.).
Securing exchanges with other organisations	Encrypt the confidential data before it is sent.
	Make sure it's the right recipient
Protect premises	Restricting access to premises through locked doors.
	Install video surveillance on site (outside buildings).
	Install intrusion alarms and check them periodically.
Cover IT developments	Provide end users with privacy-friendly settings by default.
	Avoid free comment areas or strictly frame them.
	Test on fictitious or anonymized data
	Use recognised algorithms, software, and libraries
Use cryptographic functions	Securely retain cryptographic keys

7. RIGHTS OF INDIVIDUALS

Depending on the legal basis, you can access the data concerning you, object to the processing of this data, have it rectified or, in particular conditions, have it erased. You also have the right to restrict the processing of your data. Finally, you have the right to data portability in the event of automated processing.

To exercise these rights or for any questions about this processing of your data, you can contact our Data Protection Officer electronically: dpo@utac.com

If you feel, after contacting us, that your rights are not respected or not compliant with data protection rules, you can send an online complaint to relevant regulatory authority.