Information on the processing of personal data pursuant to Article 13 of EU Regulation No. 679/2016 ("GDPR")

Dear Customer,
2B SRL (hereinafter referred to as "Data Controller") places great importance on the security and confidentiality of its Customers' personal data and wishes to provide them with information regarding the processing of their personal data.

1. DATA CONTROLLER

The data controller is **2B SRL** Via della Chiesa Campocroce, 4 – 31021 Mogliano Veneto (TV) – VAT 04495640262, (hereinafter "Controller").
For any request regarding the processing of personal data, as well as to exercise the rights recognized by the GDPR and described in point 5, the Controller can be contacted at: info@to-be.it

The Controller collects personal data from Customers for the management of normal activities provided by contracts. These personal data are processed for the following purposes:

1 - CONCLUDE CONTRACTS FOR SERVICES PROVIDED BY THE OWNER 2 - FULFILLING PRE-CONTRACTUAL, CONTRACTUAL AND TAX OBLIGATIONS ARISING FROM EXISTING RELATIONSHIPS	
Reason	The Controller needs to process certain categories of Customer personal data to respond to information requests, manage service contracts, training course registrations, and fulfill pre-contractual, contractual, and tax obligations.
Data Processed	Name and surname, personal data, tax code, address, email, phone/mobile number, banking references.
Legal Basis	Execution of a contract to which the Customer is a party (Art. 6 (1)(b) GDPR). Compliance with legal obligations (Art. 6 (1)(c) GDPR). The provision of the data is necessary, as without it, the Controller will not be able to respond to the Client's requests, or provide service communications, as well as execute the contract or contractual measures to be taken at the Client's request.
Data Retention	Customer/User data will be retained for the time necessary for the execution of the requested services, subject to further retention required by applicable regulations (e.g., Art. 2946 of the Civil Code - 10 years).
Data Sharing	- employees and collaborators of the Data Controller in their capacity as appointees and/or external data processors and/or system administrators (if appointed); - third-party companies or other entities (by way of example, credit institutions, professional firms, consultants, insurance companies, law firms, etc.) that carry out activities on behalf of the Data Controller, in their capacity as external data processors or autonomous data controllers, for the areas of reference.

3 – DEFENDING ONE'S RIGHT	
Reason	The Controller may process personal data to defend its rights and/or act in judicial, administrative, or extrajudicial proceedings related to the services provided.
Data Processed	As appropriate, personal data collected for the various purposes set forth in this policy will be processed.
Legal Basis	Legitimate interest of the Data Controller in the protection of its rights (Art. 6 (1) (f) GDPR). A new and specific provision is not required as the Controller will pursue this additional purpose, where necessary, by processing the data collected for the purposes set out in this notice.
Data Retention	Customer data with reference to the judicial protection of the Controller's rights, i.e. in case of legal obligations and/or requests of the authority will be kept for the time necessary to fulfill the legal obligation, give effect to the authority's request or pursue the protection of the right.
Data Sharing	- employees and collaborators of the Data Controller in their capacity as appointees and/or external data processors and/or system administrators (if appointed); - third-party companies or other entities (by way of example, credit institutions, professional firms, consultants, insurance companies, law firms, etc.) that carry out activities on behalf of the Data Controller, in their capacity as external data processors or autonomous data controllers for the areas of reference.

4 – COMPLIANCE WITH LEGAL OBLIGATIONS	
Reason	The Data Controller may process personal data in order to fulfill its obligations under laws, regulations or EU legislation, provisions/requirements of authorities empowered to do so by law and/or supervisory and control bodies.
Data Processed	As appropriate, personal data collected for the various purposes set out in the policy will be processed.
Legal Basis	Fulfillment of a legal obligation (Art. 6 (1) (c) GDPR). The provision of personal data for this purpose is mandatory, as failure to do so will make it impossible for the Data Controller to fulfill specific legal obligations.

Data Retention	Customer data with reference to the judicial protection of the Controller's rights, i.e. in the event of legal obligations and/or requests by the authority will be kept for as long as necessary to fulfill the legal obligation, give effect to the authority's request or pursue the protection of the right.
Data sharing	- employees and collaborators of the Data Controller in their capacity as appointees and/or external data processors and/or system administrators (if appointed); - third-party companies or other entities (by way of example, credit institutions, professional firms, consultants, insurance companies, law firms, etc.) that carry out activities on behalf of the Data Controller, in their capacity as external data processors or autonomous data controllers for the areas of reference.

5 – MARKETING ACTIVITIES	
Reason	The Controller, subject to the Client's consent, processes personal data for marketing and advertising communication purposes aimed at informing the Client about the Controller's promotional initiatives through tools such as, for example, e-mail, text messaging and other mass messaging tools, or for market research and statistics.
Data Processed	Name and surname, email, mobile/phone number.
Legal Basis	Consent (Art. 6 (1)(a) GDPR). Consent can be revoked at any time. The provision of personal data is optional; failure to provide them has no consequences for contractual relations.
Data Retention	Customer data will be retained, based on the provisions of the Guarantor's Provision 9486485 of 15.10.2020 and in any case, as long as the Customer makes use of the services of the owner and does not object to the processing in the manner provided for in Article 5 of this policy.
Data Sharing	- employees and collaborators of the Data Controller in their capacity as appointees and/or external data processors and/or system administrators (if appointed); - third-party companies or other entities carrying out activities on behalf of the Data Controller, in their capacity as external data processors or autonomous data controllers for the relevant areas.
	We point out that if you are already a customer, the Controller may send commercial communications regarding services and products of the same similar to those already used, unless the Customer disagrees (art. 130 c. 4 Privacy Code).

The updated list of data processors and processors is kept at the registered office of the Data Controller.

2. PROCESSING METHODS

The Controller processes Customers' personal data by means of the operations indicated in Art. 4 No. 2) GDPR, namely:
- collection, recording, organization, storage, consultation, processing, modification, selection, extraction, comparison, use, interconnection, blocking, communication, deletion and destruction of data.
The data are subjected to both paper and electronic processing.

The Controller retains personal data of Customers, only for as long as necessary to achieve the purposes for which it was collected or for any other related legitimate purpose.
Personal data that is no longer necessary or for which there is no longer a legal basis for its retention, will be deleted/destroyed.
If the processing of personal data fulfills more than one purpose, it will be deleted or anonymized as soon as the retention period related to the last purpose has expired.

3. TRANSFERS TO THIRD COUNTRIES

Personal data are stored at the Controller's premises, however, some service providers for software license activation require master and contact data of purchasers, specifically:

- **Pré Consulting B.V.** supplier of the SimaPro software (Netherlands) (EU)
- **Carbon Minds GmbH** supplier of the Carbon Minds database (Germany) (EU)
- **ESU-services Ltd** supplier of the ESU database (Switzerland) (EU Adequacy Decision 26.07.2000)
- **New Earth B** supplier of the SHDB database (US) (Extra EU) (EU Adequacy Decision 10.07.2023)

In this case, the Controller may transfer - depending on the service purchased - data to countries outside the European Union (EU) or the European Economic Area (EEA). In this regard, please refer to the specific privacy policies of the individual providers, who operate as autonomous controllers.

With reference to the transfer of data to the **United States**, the European Commission approved on July 10, 2023, the EU-US Data Privacy Framework (https://www.dataprivacyframework.gov/s/participant-search) which states that “the United States shall ensure an adequate level of protection, comparable to that of the European Union, for personal data transferred from the EU to U.S. companies [...].” In essence, the adequacy decision ensures that personal data of European citizens can “flow safely from the EU to U.S. companies participating in the Framework, without having to put in place additional data protection safeguards.”

This legislation is applicable to any transfer to the U.S. by electronic means, regardless of the instrument used for that transaction. Since the legislation is evolving, the risk that in certain occasional situations the U.S. public authority will operate a data access cannot be excluded.

With regard to the transfer of data to **Switzerland**, the European Commission approved on July 26, 2000 under Directive 95/46/EC, the adequacy decision establishing that Switzerland provides an adequate level of protection for personal data transferred from the EU.

In particular, the transfer of customers' personal data to non-EU countries for which an adequacy decision pursuant to Article 45.3 of the GDPR has not taken place or in the absence of adequate safeguards pursuant to Article 46 of the GDPR, takes place on the basis of the provisions of Article 49.1.b) of the GDPR, since the transfer is necessary for the performance of the contract concluded between the data subject and the data controller, or for the performance of pre-contractual measures taken at the request of the data subject.

4. DATA PROTECTION RIGHTS AND TO MAKE COMPLAINTS TO THE SUPERVISORY AUTHORITY

Each Client has the right to request from the Controller, subject to the existence of the legal prerequisite underlying the request:

a) access to personal data, as provided for in Art. 15 of the GDPR;
b) rectification or integration of personal data in the possession of the Controller deemed inaccurate, as provided for in Art. 16 of the GDPR;
c) deletion of personal data for which the Controller no longer has any legal prerequisite for processing, as provided for in Art. 17 of the GDPR;
d) the restriction of the way in which personal data are processed, if any of the cases provided for in Art. 18 of the GDPR apply;
e) the copying of personal data provided to the Controller, in a structured, commonly used and machine-readable format and the transmission of such data to another data controller (so-called portability), as provided for in Art. 20 of the GDPR
f) the revocation of consent, where the processing is based on such legal basis.

Right to object: in addition to the rights listed above, the Client may always object at any time to the processing of personal data carried out by the Controller in pursuit of its legitimate interest. In addition, the Client may always object at any time if personal data are processed for marketing purposes. The exercise of these rights, which can be done through the contact details of the Controller indicated in point 1, is free of charge and is not subject to formal constraints. It will be the responsibility of the Controller to verify that the Client is entitled to exercise the relevant right and to give feedback, as a rule, within one month. In the event that the Client believes that the processing of his/her personal data is in violation of the provisions of the GDPR, he/she has the right to lodge a complaint with the Guarantor for the Protection of Personal Data, using the references available on the website www.garanteprivacy.it, or to take appropriate legal action.

Latest update: january 2025