

Supplier Data Protection Policy

Pursuant to Art. 19 of the Data Protection Act (hereinafter also only "FADP"), Art. 13 of the Ordinance on Data Protection (hereinafter also only "OPDa"), as well as Art. 13 of the EU Regulation 679/2016 (hereinafter also only "GDPR") where applicable, Ideal-tek SA, as better identified below, as the "Data Controller" or "IDEAL-TEK" or "Company", provides you with the following information regarding the processing of personal data (i.e. any information concerning an identified or identifiable natural person) provided by you. In accordance with the regulations indicated, this processing will be based on the principles of correctness, lawfulness, transparency and protection of your privacy and rights.

Personal data controller

The personal data controller is:

Ideal-tek SA

Via Giuseppe Motta 4

6828 Balerna

represented by the persons entitled to sign in accordance with the entries in the Cantonal Trade Register (CHE-106.873.814).

The list of Data Processors and any authorized persons appointed is kept at the Data Controller's premises and made available at the request of the data subject.

Definitions

Pursuant to Section 5 of the Federal Act on Data Protection (FADP), we provide the following definitions:

- **Personal data:** all information concerning an identified or identifiable natural person;
- **Data subject:** the natural person whose personal data are being processed;
- **Processing:** any operation concerning personal data, regardless of the means and procedures used, namely the collection, recording, storage, use, modification, communication, storage, erasure or destruction of data;
- **Communication:** the transmission of personal data or making them accessible;
- **Data Controller:** the private individual or federal body which, individually or jointly with others, determines the purpose and means of the processing;
- **Data Processor:** the private individual or federal body that processes personal data on behalf of the Data Controller.

Personal data being processed

To the extent permitted by applicable regulations, the Company may process your (common) personal data collected during the management of the contractual relationship:

Specifically, the Company processes, by way of example but not limited to, the following personal data:

- personal, identification and contact data (of the data subject) such as first name, surname, nationality, address, home address, telephone number and e-mail address;
- photographic images of those concerned;
- company name where it contains personal data;
- tax domicile, other documents and tax information;
- common data of employees and/or collaborators and/or consultants of the person concerned;
- identification data of the legal representative of the interested party;
- administrative and accounting data for possible payments (e.g. IBAN, account number, and in general the information needed to make payments and invoicing);

The Company undertakes to keep the personal data of the persons concerned correct and up-to-date.

Supplier Data Protection Policy

Therefore, should your personal data change, please inform us of the change as soon as possible.

Purpose of processing

The company processes your personal data for the following specific purposes:

- Fulfil, execute, terminate the contract for the supply or provision of services and/or pre-contractual measures, and in particular to:
 - select the supplier;
 - negotiate contractual relations and request information prior to the conclusion of the contract;
 - request an offer or special prices with reference to specific projects;
 - formalize the contract;
 - fulfil any tax and social security obligations;
 - manage the commercial, contractual and financial relations established;
 - performing a service or one or more contractually agreed transactions or transactions related thereto (including issuing orders, receiving and checking the product/service);
 - meet operational or management requirements (including the management of relations with data subjects for administration, accounting, invoicing, services, management of any litigation and correspondence, management of appointments and visits);

- Fulfil all administrative tasks, if any, and in particular to
 - provide news and information related to the activity performed;
 - make, register and handle any complaints;
 - collect, record and edit supplier master data;

- transferring the personal data of data subjects to another company in connection with the transfer of a company or business unit, takeover, merger or demerger;

- verify that the activities/conduct engaged in by the person concerned do not conflict with the company's own principles/rules;

- for the verification and evaluation of the supplier;

- Organizing and managing corporate events in which stakeholders take part, aimed at strengthening the corporate identity by publicizing the company and the event on corporate social networks;

- fulfilling regulatory obligations (legal, tax or regulatory) related to the management of the contractual relationship established;

- to ensure IT security and functionality as well as SW and HW IT maintenance;

- to implement security measures for buildings and installations;

- to outsource functions and services to service providers and auxiliaries engaged by the holder;

- assert rights in judicial, extrajudicial or administrative proceedings and exercise the right of defense in legal disputes;

Supplier Data Protection Policy

- manage fulfilments related to endo societal and financial organization as well as reporting and controlling, and specifically for corporate compliance, risk management, audit and due diligence, and/or crime prevention, detection and investigation.

Legal basis and justified reason

Pursuant to Article 6 FADP, the Controller processes your personal data within the applicable legal framework. Where required, and depending on the purpose of the processing activity, the processing of your personal data may be based on one of the following legal bases/reasons:

- for processing relating to the completion and performance of the contract: overriding interest of the Data Controller, sub specie performance of the contract (Art. 31 FADP c. 2);
- for the fulfilment of regulatory obligations connected with contract management: the need to fulfil a legal or regulatory obligation (Art. 31 FADP c. 1);
- for purposes of managing the fulfilments related to the endo societal organization and specifically for corporate compliance, risk management, audit and due diligence activities, and/or crime prevention, detection and investigation; to assert rights in judicial, extrajudicial or administrative proceedings and exercise the right of defense in legal disputes;
- to guarantee IT security and functionality;
- to outsource functions and services to service providers and auxiliaries appointed by the Data Controller to implement security measures for buildings and plants;
- to transfer the personal data of data subjects to third party companies in connection with company or business unit transfers, acquisitions, mergers, demergers;
- to verify that the activities carried out by the data subject do not conflict with its business principles and rules; for the organization and management of business events;
- for supplier verification and evaluation: overriding interest of the Data Controller sub. species legitimate interest of the Data Controller (Art. 31 FADP c.2).

The provision of personal data for the purpose of the conclusion and execution of the contract is a necessary requirement and, therefore, any refusal to provide such data in whole or in part may make it impossible for the Company to execute the contract.

Where the legal basis of the processing is the legitimate interest of the Data Controller, the Data Controller guarantees that it has previously carried out an assessment ('balancing test') aimed at ensuring the proportionality of the processing so that the rights and freedoms of the Data Subjects are not adversely affected, taking into account the Data Subjects' reasonable expectations in relation to the specific processing activity performed.

In the event that the Company intends to use your personal data for any other purpose incompatible with the Purposes for which it was originally collected or authorized, the Company will inform you in advance and, where required, request your consent for such processing activities.

Modalities of personal data processing

Personal data will be processed by manual, computerized and telematic means.

Supplier Data Protection Policy

Data may be collected, recorded, stored, used, modified, communicated, archived, deleted or destroyed using instruments and procedures that guarantee security and confidentiality.

Personal data will not be processed by fully automated means, including profiling.

Conservation period

Your personal data will be stored in accordance with Art. 6 no. 4 FADP, where applicable, on the basis of the principle of necessity of processing:

- for the entire duration of the contract and, thereafter, for a period not exceeding 10 years from the termination of the contractual relationship (except for the receipt of acts interrupting the statute of limitations or the existence of the prerequisites for the suspension of the statute of limitations or the specific agreement of a different retention period between the parties or, in any case, for the different period provided for by law - for the proof of the fulfilment of legal or tax obligations or that necessary to enable the Company to possibly protect its rights in judicial or administrative proceedings or in any case before a Public Authority);
- in order to comply with legal obligations, as well as in accordance with any deadlines stipulated by specific regulations on the retention of data and documentation (cf. both tax and commercial law), as well as to comply with regulatory and/or post-contractual obligations and/or to protect your legitimate interests;
- the images of Data Subjects collected for the purposes of publicizing the company and its events on the company's social networks will be kept for the time strictly necessary for the pursuit of the purposes and in any case no longer than 10 years from their collection.

In any event, the data will be retained for the duration of the extrajudicial and/or judicial proceedings, until the time limit for judicial remedies and/or appeals is exhausted.

Subsequently, once the aforementioned reasons for processing no longer apply, the Data will be deleted or simply kept anonymous, if there are further legitimate interests of the Data Controller and/or legal obligations.

Security Measures

All Company personnel who have access to personal data are required to comply with internal rules and procedures concerning the processing of personal data in order to protect them and guarantee their confidentiality. The Controller has also implemented appropriate technical and organizational measures to protect personal data against destruction, loss, modification, misuse, disclosure or unauthorized, accidental or unlawful access, as well as against all other unlawful forms of processing.

Target audience

Your personal data may be communicated, where necessary, to:

- Data Processor;
- Natural persons acting under the authority of the Data Controller and the Data Processor for the purposes set out above;
- Firms or companies in the context of assistance and consultancy relationships (e.g. legal, auditing);
- Parties that have the right to access your data due to legal provisions, secondary or EU regulations;
- Competent authorities for the fulfilment of legal obligations and/or provisions of public bodies upon request;
- Representative in the European Union for Data Protection;
- Personal Data Protection Advisor where appointed.

Supplier Data Protection Policy

Where the data controller transfers your data to third-party service providers, the data controller shall ensure that they meet the same security standards.

Third-party service providers are therefore required to comply with a number of technical and organizational security measures, regardless of their location, including measures relating to: (i) information security management; (ii) information security risk assessment; and (iii) information security measures (e.g. physical access controls, logical access controls; malware and hacking protection; data encryption measures; backup and recovery management measures). The third parties described above must process the personal data shared under this provision in accordance with the purpose for which such data was originally collected and at least to the same level of protection as in Switzerland.

The list of Data Processors is constantly updated and available at the Data Controller's head office.

Communication of data outside the Swiss Confederation

Your personal data, processed for the purposes set out in Article 4, will be kept in Switzerland and will not be transferred to third countries that do not have the same data protection laws as the country where the information was originally provided, without the consent of the person concerned.

In view of this, the Holder has taken steps:

- by expressly requesting that Microsoft's M365 servers be located in Switzerland.;
- that the transfer of the personal data of the persons concerned to third countries (Italy) only takes place in compliance with Article 16 of the FADP, i.e. a country ensuring adequate protection, and in particular in accordance with the OPDa of 31 August 2022 (as of 15 September 2024) - Annex 1.

For the sake of completeness, it should be noted that, pursuant to Art. 16 and 17 of the FADP, the transfer of personal data may only be communicated abroad if the Federal Council has found that the legislation of the recipient state or international body guarantees adequate data protection, or if the data subject has given his or her consent; the communication is directly related to the conclusion or performance of the contract; the communication is necessary for the protection of an overriding public interest or for establishing, exercising or asserting a right before a court or a competent foreign authority; the communication is necessary to protect the life or physical integrity of the data subject or a third party; the data subject has made the personal data accessible to anyone; the data originates from a register provided for by law that is accessible to the public or to persons with an interest worthy of protection.

Your personal data will not be subject to dissemination or to any fully automated decision-making process, including profiling.

Rights of the data subject

Pursuant to the FADP, the Holder acknowledges in particular the following rights (non-exhaustive list):

- to be subject to transparent processing (Art. 19-21 FADP and 12 GDPR);
- to obtain confirmation as to whether or not personal data is being processed and, if so, to obtain access to the personal data - including a copy thereof - and communication of, among others, the following information: purpose of the processing, categories of personal data processed, recipients to whom the data has been or will be communicated, period of data retention, (right of access - Article 25 of the FADP and 15 GDPR)
- obtain, without undue delay, the rectification of inaccurate personal data and/or the supplementation of incomplete personal data (right of rectification - Article 32(1), (3) and (4) of the FADP and 16 GDPR)
- to obtain, without undue delay, the erasure of personal data (right to erasure - Article 32(2)(c) of the FADP and 17 GDPR)

Supplier Data Protection Policy

- receive, in a structured, commonly used and machine-readable format, personal data where the processing is based on consent and is carried out by automated means (right to data portability - Article 28 of the FADP and 20 GDPR);
- object to the processing at any time, for reasons related to their situation (right to object - Article 30 2 letter B and 3 FADP and 21 GDPR). If this right is exercised, the Company will refrain from further processing of personal data, provided that there are no compelling legitimate grounds to proceed with the processing anyway;
- obtain the restriction of processing (right to restriction of processing) where the accuracy of personal data is contested (for the period necessary for the Data Controller to verify the accuracy of the personal data) or where the data subject has objected to the processing (pending verification as to whether the Data Controller's legitimate reasons prevail over those of the data subject) (Art. 18 GDPR)
- to obtain the possibility of asserting one's point of view with respect to automated decisions and in particular that of demanding a review of the decision by a human being (right not to be subject to an automated individual decision - Art. 21 FADP and 22 GDPR)
- to lodge a complaint with the competent supervisory authority (in Switzerland the Federal Data Protection and Information Commissioner - FDPIC);
- if neither the correctness nor the inaccuracy of the personal data can be proven, request that a note be added to indicate the dispute;
- request that the rectification, destruction, blocking, especially communication to third parties, in addition to the note on the objection or ruling be communicated to third parties or published;
- have the processing of personal data declared unlawful.

The data subject may exercise his or her rights in the following ways:

- **by e-mail:** sending a request to the Company to the following e-mail address: privacy@ideal-tek.com
- **by post:** Ideal-tek SA, Via Giuseppe Motta 4, 6828 Balerna.

Data subjects in the European Union can exercise their rights by contacting the representative in the European Union at the contact details provided in Art. 13.

When contacting the Data Controller, you should make sure to include your name, e-mail address, postal address and/or telephone number(s) to ensure that the Data Controller can handle your request correctly.

The Company will comply with such requests, revocations or objections as required by applicable data protection regulations at the latest within one month of receipt of the request. This deadline may be extended depending on the complexity or number of requests and the Company will explain to you the reason for the extension.

Privacy contact person

The Company has appointed a privacy contact person, who can be contacted at the Data Controller's address above or by sending an e-mail to privacy@ideal-tek.com.

Updating this policy

The Controller reserves the right to change, update, add or remove parts of this privacy policy at its own discretion and at any time.

Effective Date, December 1st 2024