Visitors Privacy Policy

In accordance with Art. 19 of the Federal Act on Data Protection (hereinafter also only "FADP"), Art. 13 of the Data Protection Ordinance (hereinafter also only "OPDa"), Ideal-tek SA (hereinafter also only "Ideal-tek" or "Company" or "Controller") as better identified below, as Data Controller, provides you with the following information regarding the processing of your personal data (i.e. any information concerning an identified or identifiable natural person) that you provide when accessing the Company's premises. Visitors are understood to be all employees of external companies with which the Company has professional relations and who, on an ad hoc or continuous basis for a specific period of time, must have access to the Company's offices. The category of visitors also includes employees and/or collaborators of the Company's outsourcers, external auditors, employees of companies required to perform maintenance work on the building, employees and collaborators of existing and/or potential counterparties, employees and/or collaborators of suppliers, cleaning staff and customers. The types of visitors are therefore, by way of example, the following: customers, counterparties, IT technicians and cleaning staff, consultants, workers/technicians/craftsmen.
In accordance with the regulations indicated, this processing will be based on 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 law, the Company may process the following personal data collected during your access to the Company's premises:

- personal and identifying data such as name, surname, company, telephone number;
- date, time of entry and time of exit;

- images from the installed video surveillance system where your passage is detected within the range of the cameras.

The Company undertakes to keep your personal data correct and up-to-date.
The personal data processed by the Company are acquired directly from the person concerned.

Purpose of processing

Your personal data will be processed by the Company for the following purposes:

- allow access to the Company and its offices upon verification of the identity of outsiders;
- affirming and guaranteeing the security of persons accessing the Company in various capacities, as well as for the protection of the Company's assets and thus of its premises and property from theft, vandalism or unauthorised access and, more generally, to protect the Company's know-how;
- to transfer the personal data of the persons concerned to another company in connection with the transfer of a company or business unit, takeover, merger or demerger;
- assert rights in judicial, extrajudicial or administrative proceedings and exercise the right of defence in legal disputes.

Legal basis and justification

In accordance with 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 grounds:

- for processing relating to the recording of accesses, for the processing of images for the purpose of protecting persons, company property and the company's assets in connection with the installed video-surveillance system, as well as for asserting rights in judicial, extrajudicial or administrative proceedings and exercising the right of defence in legal disputes, and for transferring the data subject's data to third-party companies in connection with company or business unit transfers, mergers, demergers or acquisitions: overriding interest of the Data Controller (Art. 31 FADP c.2).

The provision of personal data is a necessary requirement for access to the Company's premises, and therefore any refusal to provide it in whole or in part may result in the impossibility of access to the Company.
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 that is incompatible with the Purposes for which it was originally collected or authorised, the Company will inform you in advance and, where required, request your consent for such processing activities.

Personal data processing methods

Personal data will be processed by manual, computerized and telematic means, with and without the aid of automated means.

Visitors Privacy Policy

Data may be collected, recorded, stored, used, modified, communicated, archived, deleted or destroyed using instruments and procedures that guarantee security and confidentiality.
Your personal data will not be subject to any fully automated decision-making process, including profiling.

Retention Period

We will only store your personal data for as long as it is necessary to achieve the purpose for which it was collected.
With regard to the images inherent to the video surveillance system, they will be viewed in real time by authorised operators as well as recorded through the video surveillance systems. Specifically, they will be collected as soon as the person concerned enters the video-surveillance area, recognizable through the presence of appropriate signage, and will be stored for a period not exceeding one month, as set out in the video-surveillance system management procedure.
In any case, the Data will be retained for the entire duration of the extrajudicial and/or judicial proceedings, until the exhaustion of the time limits for judicial protection and/or appeal actions. Subsequently, should the aforementioned reasons for processing cease to exist, the Data will be deleted, destroyed or simply kept anonymous.

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 ensure their confidentiality. We have 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.

Recipients

Your personal data may be communicated, where necessary, to the following recipients:

- Responsible;
- 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);
- parties that have the right to access your data due to legal provisions, secondary or EU regulations;
- subjects that provide services for the management of the information system used by the Company and the telecommunications networks;
- Authorities competent to fulfil legal obligations and/or provisions of public bodies upon request, including prosecuting authorities.
-

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 organisational 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.

In view of this, the Data Controller has taken steps:

✓ expressly requesting that Microsoft's M365 servers be located in Zurich.

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 organization guarantees adequate data protection, or if the data subject has given his or her consent; the communication is directly related to the conclusion or execution 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.
Nor will your personal data be subject to dissemination or to any fully automated decision-making process, including profiling.

Rights of the data subject

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

- Be subject to transparent treatment (Art. 19-21 FADP);
- to obtain confirmation as to whether or not personal data are being processed and, if so, to obtain access to the personal data - including a copy thereof - and communication of, inter alia, the following information: the purpose of the processing, the categories of personal data processed, the recipients to whom the data have been or will be disclosed, the period for which the data are to be retained, (right of access - Article 25 of the FADP);
- obtain, without undue delay, the deletion of personal data (right to erasure - Article 32(2)(c) of the FADP) or the deletion of recordings and, if necessary, to change the angle of the recording or the position of the cameras;
- object to the processing at any time, on grounds relating to their situation (right to object - Article 30 2 lit. B and 3 FADP). If this right is exercised, the Company will refrain from any further processing of personal data, provided that there are no compelling legitimate grounds for processing anyway;

Visitors Privacy Policy

- file a complaint with the competent supervisory authority (in Switzerland the Federal Data Protection and Information Commissioner - FDPIC);

The person concerned may exercise his or her rights in the following ways:

– by e-mail: by sending a request to the company at the following e-mail address: privacy@ideal-tek.com.

– by ordinary post to the registered office of the Company: Ideal-tek SA, Via Giuseppe Motta 4, 6828 Balerna.

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 the applicable data protection regulations at the latest within one month after receipt of the request. This deadline may be extended depending on the complexity or number of requests and the Company will explain the reason for the extension.

Privacy contact

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 01.12.2024