# Privacy Notice for Employees

## 1 What is this privacy notice about?

Implenia AG and its affiliated subsidiaries and Group companies (hereinafter referred to as Implenia) would like to inform you about how we internally process your data from the initiation of the contract, during the employment relationship and possibly beyond. This privacy notice applies in addition to our general privacy notice, which you can find here. In the latter, you are informed about how and for what purpose your personal data is processed in connection with our websites, among other things. This privacy notice complies with the EU General Data Protection Regulation ("GDPR") and the Swiss Data Protection Act ("DSG"). However, the application of these laws depends on each individual case.

Integrity is a special value for Implenia and part of our mission statement (Mission Statement Implenia - Implenia Ltd.), so we have attempted to present the following to you as clearly and transparently as possible. If, despite all our efforts, there are still any uncertainties, please do not hesitate to contact us.

## 2 Who is responsible for processing your Data?

The specific Implenia Group company responsible for collecting and processing your data is the company that is your employer in your employment contract. You can contact this specific Implenia Group company at any time for data protection concerns and to exercise your rights in accordance with section 9. A list with all locations and their respective responsible contact is available here.

If you have any questions or concerns about data protection at Group level, or if you are not sure which organisation you are allocated to, please contact:

Implenia AG
Thurgauerstrasse 101 A
8152 Glattpark (Opfikon)
Switzerland
dataprivacy@implenia.com

In addition, a data protection officer has been appointed for the Group companies in Germany in accordance with Article 37 et seq. GDPR and Section 38 of the Federal Data Protection Act (BDSG), who can be contacted as follows:

Implenia Deutschland GmbH
Data Protection Officer(s)
Am Prime Parc 1
65479 Raunheim
Germany
dataprivacy-germany@implenia.com

## 3 What Data do we process and for what purpose?

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

- Initiation of the employment relationship,
- Implementation and termination of the employment relationship,
- Use and application of work results,
- Health care,
- Behavioural and performance assessment,
- Team and organisational development,
- Employer's obligations that go beyond the employment relationship.

We process different categories of data about you, including current but also previous versions where information may change over time. The main categories of data are:

***(The examples of application given do not necessarily apply to every employee and may differ slightly depending on the country of employment due to other legal requirements).***

### 3.1 Employee Master Data

We refer to employee master data as the basic data that we require in addition to financial data to comply with our duties under the employment contract and statutory reporting obligations. This includes, for example, data such as name, address, email address, telephone number and other contact details, gender, date of birth, nationality, social facts, bank details, national insurance number, pension insurance number, tax number, etc.

Special categories of data may be involved (e.g., infirmity status, health data for the assessment of your ability to work, in the context of occupational reintegration management or trade union membership).

### 3.2 Working Hours and Absence Data

Furthermore, we process data on presences and absences, such as time recording data, holiday periods, etc. Distinctive categories of data may be affected (e.g., periods of inability to work, accident related data).

### 3.3 Financial Data

In connection with the payment of your salary, company allowances and other benefits, we collect data concerning your payment and bank details, tax information and other information required for payroll administration, tax deduction and any other benefits. We generally keep this data for the duration of the employment relationship as well as for the period stipulated by law. Financial data such as your salary and related information (e.g., payslips, social security contributions, family allowances, bonuses, premiums, shares in the Implenia Group company and information about your basic salary and salary level), information about other benefits (e.g., travel benefits and allowances and information about the deduction of withholding taxes) and expenses (e.g., the use of credit cards, expense claims and reimbursements, including those in connection with business trips). In the event of a wage/salary garnishment, we will be informed by the official authority in charge. In this case, we must pay all or part of your salary to the authority and process the related information.

### 3.4 Technical Data

When you use our corporate network, IT systems, internal platforms, applications and tools (e.g., Intranet, Implenia support systems, ERP systems, business applications, mobile devices and other collaboration and communication tools) or other infrastructure (e.g., building or property access systems), we will inevitably collect data about your logins, accesses and exits building or property access systems, we will necessarily collect data about the credentials you provide, your logins, file accesses, building entries and exits, your use of our applications, systems and other infrastructure and electronic devices, and data about the devices, equipment and other tools you may use to ensure the functionality and security of those services, systems and other infrastructure. Where necessary for an audit trail or statistical purposes, we will also log this data. Such technical data may be linked or matched to other categories of data (and possibly to you as a person) in connection with your employee user account, access controls or performance of the employment contract (e.g., to verify your identity or access rights). Technical data includes information about the device you are using (operating system, unique identifiers, applications, browsers), data used to authenticate you as an authorised user (usernames, passwords), but also certain actions (your logins, use of certain applications and functions, files you access, calls made or received, web pages you access, emails you send or receive). Of course, this data will not be further analysed by the employer! Some applications (e.g., accounting systems) track all the data you enter, change or delete to create an audit trail.
This information is usually linked to you because we generally only allow authenticated users to use our systems, accordingly you should never share your login details with anyone else. We do not collect keystrokes or similar information. We try to limit audit trails to those that are necessary for the operation and security of our IT systems and applications and for other authorized purposes. However, we may collect additional technical data that we would not otherwise collect in the event of reasonable suspicion of a serious compliance breach, a criminal investigation or due to legal obligations, subject to applicable law.

### 3.5 User Account Data

This is the data we collect and store about you so that you can log into our systems, access our buildings, identify, authenticate yourself to third parties and have your "personal" area in our computer systems (e.g., your mailbox). User account data typically includes your name, any contact and organisational information, access rights and, in the context of access control systems, biometric data if applicable. The storage period may be extended if this is necessary for reasons of evidence, to meet legal or contractual requirements or for technical reasons. Please note that your account data may be logged in the form of technical data (see above) and may contain preference data (see below). The contents of your mailbox are usually considered communication data (see below), and business-related contents of the personal area are usually work result data (see below). Account data includes data such as usernames, passwords, phone numbers for multi-factor authentication, access rights and permissions, access badge information and company IDs. If biometric data is collected for access control purposes, you will be informed separately.
We either collect this information directly from you or create it based on information you have provided to us. In relation to computer accounts and network accounts and access control permissions, the data is replicated within the respective systems. If third parties (e.g., customers, business partners, service providers, etc.) need to identify or authenticate you for work purposes, we may also share this information with them. With respect to our computer systems, your account also serves as a location for storing personal data, preference data, communication data and other information that is personal or possibly even of private nature (e.g., if you store a private document in your "personal" folder on the corporate network). In addition, all documents that you have placed on your computer "desktop" are stored in your account.

### 3.6 Communication Data

We may record (video) conferences via Microsoft Teams to preserve know-how, for quality assurance and training purposes. You will be informed of such recordings by a notification in MS Teams when a recording is made. Communications relevant to our mutual employment relationship may be kept (e.g., in the HR file) for the duration of the relationship. As an employee, the communications data includes all your business communications (e.g., emails you send or receive). If you are in contact with other employees of the Implenia Group, our support areas (e.g., HR and IT support) or third parties (e.g., clients, suppliers, business partners, etc.) via group chat or messaging applications, your work email address, telephone number or other company communication tools, we assume that this communication is work-related and as such, collect the data exchanged, including the metadata of the communication. If you use company communication tools for private communication, we will inevitably also automatically collect these private communications in our IT systems. Communication data includes your name and contact details, means, place and time of the communication and usually also its content (e.g., content of emails, letters, internal chats, etc.). This data may also include information about third parties (e.g., clients, suppliers, business partners and family members). Communication data may also occur as technical data or account data.

### 3.7 Qualification Data

Data from your original application (such as CV, cover letter, diplomas, certificates, performance records and letters of recommendation) will be retained as part of your personnel file for the duration of your employment. This period may be extended if necessary for reasons of proof, compliance with contractual or legal requirements (incorporating local applicable laws) or for technical reasons.

Qualification data includes basic data: information about your academic background, diplomas, certificates, academic performance records, technical skills, certificates of suitability and qualification, language skills, work history (including job titles), reference information from third parties (where permitted) and extracurricular activities, name of relatives employed by Implenia, if applicable, and salary and wage expectations.

Qualification data also includes evaluations and reports about you as an employee that aim to continuously assess or confirm your suitability for the position you hold.

### 3.8 Administrative Data

At the beginning of your employment with us and throughout the duration of our engagement with you, we collect data about you that enables us to administer and manage our mutual employment relationship, prepare our

workplace facilities for you and assign you to an organisational unit and team. Administrative data includes data such as your job and employment contract details (e.g., job, title, function, organisational unit, migration status, marital status, professional association membership, military status, passport number, contract start and end dates, starting salary, number of days of leave, schedules including night and weekend work, etc.), your place of work (including home office information), your professional contact details (e.g., professional postal address, email address and team), your photo (e.g., for the intranet and our website), information about your team (e.g., your superiors, your direct reports, mentors, subordinates and other team members) and your emergency contacts (e.g., your spouse, next of kin and children) and their contact details (e.g., your name, date of birth, address and telephone number).

We process your photos and videos on the basis of our legitimate interest or, if applicable, on the basis of your consent.

### 3.9 Performance and Training Data

We collect data on your work performance, your disciplinary records and training and development needs. We generally retain this data for the duration of the employment relationship and for ten years after termination of the employment relationship. Performance data includes data about your performance in the workplace (e.g., probationary period appraisals, performance development appraisals, promotions, details of targets achieved and client recommendations and feedback during employment or work), involvement in work-related associations and organisations, whistleblowing notices (if you do not wish to remain anonymous) you raised or in which you may be involved or a witness of, disciplinary records (e.g., details of disciplinary or appeals proceedings you have been involved in, including any warnings or penalties imposed on you and related correspondence) and details of any change or termination of employment contract, including termination of employment or engagement. Training data includes information about your training (e.g., participation in internal and external training related to your role) and your training needs (e.g., enrolment in an advanced master's programme, participation in a secondment programme, etc.).

### 3.10 Work Product Data

We collect data, in connection with the work and content that you or others create for or share with us during your employment, that relates to you or your role working for or on behalf of Implenia within Implenia. The time we retain such work product depends on how long we need to retain them, as created or produced in the course of your work for Implenia, and the personal data processed is usually of a secondary nature. For details about your communications sent and received for business purposes, see Communications Data. Work Product Data includes all content that you or others create or process for us, or other creation or processing you are involved in, or that you share with us during your employment and that relates to you or your role working for or on behalf of Implenia within Implenia (e.g., references to you in presentations, memoranda, meeting minutes, reports, drawings, graphics, sketches, company publications, official documents, contracts, etc.), whether or not such content is protected by intellectual property laws. Many would not even consider such information as personal data, but since you may appear in such work products in an identifiable way, we list it here anyway. No personal profiling takes place when processing your data.

## 4 On what basis do we process your Data?

Unless we ask for your consent, the processing of your personal data is based on handling it for the initiation, performance, or termination of an employment contract with you or on our legitimate interest in the respective processing.

If we ask for your consent for certain processing activities (e.g., for the processing of sensitive personal data), we will inform you separately about the respective processing purposes. Consent is always voluntary, so you can withdraw your consent at any time with future effect by notifying us in writing (post or email); once we have received notification of the withdrawal of consent, we will no longer process your data for the purpose(s) to which you consented, unless we have another legal basis to do so. However, withdrawal of consent will not affect the legitimacy of processing carried out on the basis of consent prior to withdrawal. If you withdraw your consent to the processing of personal data, it follows that the purpose for which it was given cannot be further pursued.

In certain circumstances, we may process data collected based on other legal grounds, e.g., in the event of a dispute, where this is necessary in connection with a potential legal dispute or for the enforcement or defence of legal claims. In some cases, a different legal basis may apply, which we will inform you of separately if necessary.

## 5 Who do we share your Data with?

We work with service providers in the EEA (European Economic Area), Switzerland and other countries who process your data on our behalf or as joint controllers with us or receive data concerning you as appointed controllers. This may include health data. To optimise our IT systems and internal applications and tools and to focus on our core competencies, we procure services from third parties in various areas. These include IT services, information transfer, communication services and services from recruitment agencies and staffing companies. We share the data that these providers need to fulfil their services. They may also use this data for their own purposes, for example anonymised information to improve their services. In addition, we conclude contracts with these providers to ensure compliance with data protection, insofar as this does not result directly from the law (e.g., authorities).

For our (video) conferences, we use Microsoft Teams from Microsoft Ireland Operations Limited. Where we are the data controller, we only process and share data with Microsoft that is necessary to use the features of Microsoft Teams (e.g., your email address to send you an invitation). Microsoft may also collect data about you to provide their services to us (e.g., recording conferences) and use it for their own purposes. More information about how Microsoft processes your data given here:

Microsoft Teams Privacy - Microsoft Teams | Microsoft Learn

## 6 In which countries does your personal Data end up?

As explained in section 5, we share data with other parties. These are not all located in the EEA and in Switzerland. Your data may therefore also be processed in further countries, exceptionally in any country in the world. If a recipient is located in a country without adequate legal data protection, we oblige them to comply with the applicable data protection law (for this purpose we use the European Commission's standard contractual clauses, which are accessible here) unless they are already subject to legally recognised regulations to ensure data protection and we do not rely on an exemption. An exception may apply in the case of legal proceedings abroad, but also in cases of overriding public interests or if the performance of a contract requires such disclosure, if you have consented or if it is a matter of data that you have made generally accessible and the processing of which you have not objected to.

## 7 How long do we process your Data?

We process your data as long as our processing purposes, the legal retention periods and our legitimate interest in documentation or evidence require it, or your consent is valid.

Documentation and evidence purposes include our interest in documenting our interactions and other facts relating to the performance of the employment contract in relation to legal claims, discrepancies, IT, infrastructure security requirements and demonstrating good Corporate Governance and Compliance. Retention may also be a technical requirement where certain data cannot be separated from other data and we therefore need to keep it (e.g., backups or document management systems).

## 8 How do we protect your Data?

We take appropriate security measures to maintain the confidentiality, integrity and availability of your personal data, to protect it against unauthorised or unlawful processing and to protect it against the risks of loss, unintentional alteration, unauthorised disclosure or access.

## 9 What rights do you have?

Applicable data protection laws give you the right to object to the processing of your data under certain circumstances, in particular for processing actions based on legitimate interest.
To help you control the processing of your personal data, you have the following rights in relation to our data processing, depending on the applicable data protection law:

- the right to request information from us as to whether and what data of yours we process;
- the right to have data corrected by us if it is inaccurate;
- the right to request that we delete data;
- the right to request that certain personal data is provided to you in a commonly used electronic format or have it transferred to another controlling instance;
- the right to withdraw your consent where our processing is based on your consent;
- the right to obtain, upon request, further information useful for the exercise of these rights.

If you wish to exercise any of the above rights against us or any of our Group companies, please contact us in writing addressed to our premises or, unless otherwise stated or agreed, by email; our contact details are given in section 2. In order for us to be able to prevent abuse, we will need to identify you (e.g., by means of a copy of an identity document, if identification is otherwise not possible).

If you are in the EEA or Switzerland, you also have the right to file a complaint with the responsible data protection supervisory authority in your country.

A list of authorities in the EEA is available here: Members | European Data Protection Board (europa.eu).
You can contact the Swiss supervisory authority as follows: Contact (admin.ch).