

Data Protection Statement of mynatix ag

Version effective as of 24 May 2024

With this Data Protection Statement we, the mynatix ag (and all subsidiaries of the company) (hereinafter together **mynatix, we** or **us**), describe how we collect and further process personal data. This Data Protection Statement is not necessarily a comprehensive description of our data processing. It is possible that other data protection statements (or similar documents) are applicable to specific circumstances.

The term "personal data" in this Data Protection Statement shall mean any information that identifies, or could reasonably be used to identify any person.

If you provide us with personal data of other persons (such as family members, work colleagues), please make sure the respective persons are aware of this Data Protection Statement and only provide us with their data if you are allowed to do so and such personal data is correct.

This Privacy Notice is aligned with the EU General Data Protection Regulation («**GDPR**»), the Swiss Data Protection Act («**DPA**») and the revised Swiss Data Protection («**revDPA**»). However, the application of these laws depends on each individual case.

Controller

The "controller" of data processing as described in this data protection statement (i.e. the responsible person) is Dr. Andreas Gartmann (unless we have informed you differently in certain cases). You can notify us of any data protection related concerns, irrespective of the concerned affiliate company of mynatix ag, using the following contact details: mynatix ag, Picassoplatz 8, 4052 Basel, Switzerland; e-mail andres.gartmann@mynatix.com.

Collection and Processing of Personal Data

We primarily process personal data that we obtain from our clients and other business partners as well as other individuals in the context of our business relationships with them or that we collect from users when operating our websites, apps and other applications.

Insofar as it is permitted to us, we obtain certain personal data from publicly accessible sources (e.g., debt registers, land registries, commercial registers, press, internet) or we may receive such information from affiliated companies of mynatix ag, from authorities or other third parties. Apart from data you provided to us directly, the categories of data we receive about you from third parties include, but are not limited to, information from public registers, data received in connection with administrative or court proceedings, information in connection

with your professional role and activities (e.g., in order to conclude and carry out contracts with your employer), information about you in correspondence and discussions with third parties, credit rating information (if we conduct business activities with you personally), information about you given to us by individuals associated with you (family, consultants, legal representatives, etc.) in order to conclude or process contracts with you or with your involvement (e.g. references, your delivery-address, powers of attorney), information regarding legal regulations such as anti-money laundering and export restrictions, bank details, information regarding insurances, our distributors and other business partners for the purpose of ordering or delivering services to you or by you (e.g., payments made, previous purchases), information about you found in the media or internet (insofar as indicated in the specific case, e.g. in connection with job applications, media reviews, marketing/sales, etc.), your address and any interests and other socio-demographic data (for marketing purposes), data in connection with your use of our websites (e.g., IP address, MAC address of your smartphone or computers, information regarding your device and settings, cookies, date and time of your visit, sites and content retrieved, applications used, referring website, localization data).

Purpose of Data Processing and Legal Grounds

We primarily use collected data in order to conclude and process contracts with our clients and business partners, in particular in connection with our business activity with our clients and the procurement of products and services from our suppliers and subcontractors, as well as in order to comply with our domestic and foreign legal obligations. You may be affected by our data processing in your capacity as an employee of such a client or business partner.

In addition, in line with applicable law and where appropriate, we may process your personal data and personal data of third parties for the following purposes, which are in our (or, as the case may be, any third parties') legitimate interest, such as:

- providing and developing our products, services and websites, apps and other platforms, on which we are active;
- communication with third parties and processing of their requests (e.g., job applications, media inquiries);
- review and optimization of procedures regarding needs assessment for the purpose of direct customer approach as well as obtaining personal data from publicly accessible sources for customer acquisition;
- advertisement and marketing (including organizing events), provided that you have not objected to the use of your data for this purpose (if you are part of our customer base and you receive our advertisement, you may object at any time and we will place you on a blacklist against further advertising mailings);

- market and opinion research, media surveillance;
- asserting legal claims and defense in legal disputes and official proceedings;
- prevention and investigation of criminal offences and other misconduct (e.g. conducting internal investigations, data analysis to combat fraud);
- ensuring our operation, including our IT, our websites, apps and other appliances;
- video surveillance to protect our domiciliary rights and other measures to ensure the safety of our premises and facilities as well as protection of our employees and other individuals and assets owner by or entrusted to us (such as e.g. access controls, visitor logs, network and mail scanners, telephone recordings);
- acquisition and sale of business divisions, companies or parts of companies and other corporate transactions and the transfer of personal data related thereto as well as measures for business management and compliance with legal and regulatory obligations as well as internal regulations of mynatix ag.

If you have given us your consent to process your personal data for certain purposes (for example when registering to receive newsletters or carrying out a background check), we will process your personal data within the scope of and based on this consent, unless we have another legal basis, provided that we require one. Consent given can be withdrawn at any time, but this does not affect data processed prior to withdrawal.

Cookies, Tracking and Other Techniques Regarding the Use of our Website

We typically use "cookies" and similar techniques, if any, on our websites, which allow for an identification of your browser or device. A cookie is a small text file that is sent to your computer and automatically saved by the web browser on your computer or mobile device, when you visit our website. If you revisit our website, we may recognize you, even if we do not know your identity. Besides cookies that are only used during a session and deleted after your visit of the website ("session cookies"), we may use cookies in order to save user configurations and other information for a certain time period ("permanent cookies"). Notwithstanding the foregoing, you may configure your browser settings in a way that it rejects cookies, only saves them for one session or deletes them prematurely. Most browsers are preset to accept cookies. We use permanent cookies in order to understand how you use our services and content. Certain cookies might be sent to you from us, others from business partners with which we collaborate. If you block cookies, it is possible that certain functions are no longer available to you.

By using our websites and consenting to the receipt of newsletters and other marketing e-mails you agree to our use of such techniques. If you object, you must configure your browser or e-mail program accordingly.

In addition, we use plug-ins from social networks such as Twitter or LinkedIn on our websites. This is visible for you (typically based on the respective symbols). We have configured these elements to be disabled by default. If you activate them (by clicking on them), the operators of the respective social networks may record that you are on our website and where on our website you are exactly and may use this information for their own purposes. This processing of your personal data lays in the responsibility of the respective operator and occurs according to its data protection regulations. We do not receive any information about you from the respective operator.

Datatransfer and Transfer of Data Abroad

In the context of our business activities and in line with the purposes of the data processing set out in Section 0, we may transfer data to third parties, insofar as such a transfer is permitted and we deem it appropriate, in order for them to process data for us or, as the case may be, their own purposes. In particular, the following categories of recipients may be concerned:

- our service providers (within the mynatix group or externally, such as e.g. banks, insurances), including processors (such as e.g. IT providers);
- dealers, suppliers, subcontractors and other business partners;
- clients;
- domestic and foreign authorities or courts;
- the media;
- the public, including users of our websites and social media;
- competitors, industry organizations, associations, organizations and other bodies;
- acquirers or parties interested in the acquisition of business divisions, companies or other parts of the mynatix group;
- other parties in possible or pending legal proceedings;
- affiliates of the mynatix group;

together **Recipients**.

Certain Recipients may be within Switzerland but they may be located in any country worldwide. In particular, you must anticipate your data to be transmitted to any country in which the mynatix-Group is represented as well as to other countries in Europe and the USA where our service providers are located (such as Microsoft).

If a recipient is located in a country without adequate statutory data protection, we require the recipient to undertake to comply with data protection (for this purpose, we use the revised European Commission's standard contractual clauses, which can be accessed here: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?), unless the recipient is subject to a legally accepted set of rules to ensure data protection and unless we cannot rely on an exception. An exception may apply for example in case of legal proceedings abroad, but also in cases of overriding public interest or if the performance of a contract requires disclosure, if you have consented or if data has been made available generally by you and you have not objected against the processing.

Retention Periods for your Personal Data

We process and retain your personal data as long as required for the performance of our contractual obligation and compliance with legal obligations or other purposes pursued with the processing, i.e. for the duration of the entire business relationship (from the initiation, during the performance of the contract until it is terminated) as well as beyond this duration in accordance with legal retention and documentation obligations. Personal data may be retained for the period during which claims can be asserted against our company or insofar as we are otherwise legally obliged to do so or if legitimate business interests require further retention (e.g., for evidence and documentation purposes). As soon as your personal data are no longer required for the above-mentioned purposes, they will be deleted or anonymized, to the extent possible. In general, shorter retention periods of no more than twelve months apply for operational data (e.g., system logs).

Data Security

We have taken appropriate technical and organizational security measures to protect your personal data from unauthorized access and misuse such as internal policies, training, IT and network security solutions, access controls and restrictions, encryption of data carriers and transmissions.

Obligation to Provide Personal Data To Us

In the context of our business relationship you must provide us with any personal data that is necessary for the conclusion and performance of a business relationship and the performance of our contractual obligations (as a rule, there is no statutory requirement to provide us with data). Without this information, we will usually not be able to enter into or carry out a contract with you (or the entity or person you represent). In addition, the website cannot be used unless certain information is disclosed to enable data traffic (e.g. IP address).

Your Rights

In accordance with and as far as provided by applicable law (as is the case where the GDPR is applicable), you have the right to access, rectification and erasure of your personal data, the right to restriction of processing or **to object to our data processing, in particular for direct marketing purposes and for other legitimate interests in processing** in addition to right to receive certain personal data for transfer to another controller (data portability). Please note, however, that we reserve the right to enforce statutory restrictions on our part, for example if we are obliged to retain or process certain data, have an overriding interest (insofar as we may invoke such interests) or need the data for asserting claims. If exercising certain rights will incur costs on you, we will notify you thereof in advance. We have already informed you of the possibility to withdraw consent in Section 0 above. Please further note that the exercise of these rights may be in conflict with your contractual obligations and this may result in consequences such as premature contract termination or involve costs. If this is the case, we will inform you in advance unless it has already been contractually agreed upon.

In general, exercising these rights requires that you are able to prove your identity (e.g., by a copy of identification documents where your identity is not evident otherwise or can be verified in another way). In order to assert these rights, please contact us at the addresses provided in Section 1 above.

In addition, every data subject has the right to enforce his/her rights in court or to lodge a complaint with the competent data protection authority. The competent data protection authority of Switzerland is the Federal Data Protection and Information Commissioner (<http://www.edoeb.admin.ch>).

Amendments of this Data Protection Statement

We may amend this Data Protection Statement at any time without prior notice. The current version published on our website shall apply. If the Data Protection Statement is part of an agreement with you, we will notify you by e-mail or other appropriate means in case of an amendment.