Applixure Services Privacy Policy

Updated: September 2026

General

Applixure is committed to protect the privacy of individual persons using the Services. This Privacy Policy governs the use of Applixure services ("Services"), including any forums, technology, information, data, software and materials Applixure makes available as part of, or in connection with the Services, and helps to understand what Personal Data Applixure collects, and how such data is used.

"Personal Data" refers to data which allows the identification of an individual person (as defined in the European Union's General Data Protection Regulation 2016/679).

"Non-Personal Data" refers data that cannot be used to specifically identify any individual person.

We commit to adhere to the provisions of the aforementioned legislation and other such applicable laws and regulations pertaining to processing of Personal Data.

How Applixure collects information

Applixure will only collect such Personal Data that is relevant for the purposes described in this Privacy Policy.

Personal Data is collected directly from the use of our Services. Personal data may include: 1) Information provided by Customer and required for the provision of our products and services, including registration information (name, user name and email address for the users of the Services) and information entered into our system when using the Services. 2) Other information necessary for maintaining the customer relationship, such as billing information, feedback and marketing preferences.

By signing up for any newsletter or other email communications, or by answering any surveys on Applixure website, you will need to provide valid email address to Applixure for communication to happen. These email addresses are processed by Applixure as part of the direct marketing communication.

As part of the Services registration, or later on while using the Services when adding additional Users (as defined in the Terms of Service), Users will need to provide names and email address for each of the User account. Email addresses related to the User Accounts are primarily used for system communication purposes, such as when resetting the password or for sending out messages from the Services but can be used by Applixure when communicating changes in the Services.

When entering into agreement with Applixure, you may provide Applixure or to a designated third party payment processor with payment details in order for Applixure to provide Order Confirmation and enable valid Subscription Period.

Data sources

The Personal Data is mainly collected directly from the data subjects themselves, for example, in connection with preparing or signing of a contract or during a customer relationship. The Personal Data may also be collected automatically when the data subject uses our various products and services. In addition, and with the permission of the data subject, data may be collected in other ways in a marketing context. Personal Data may be updated and supplemented by collecting data from private and public sources.

Retention of Personal Data

Applixure retains the Personal Data pursuant to this Privacy Policy for the period necessary to fulfil the purposes outlined in this Privacy Policy unless a longer retention period is required or permitted by law. Thereafter, if the collected Personal Data is no longer needed for purposes specified in this Privacy Policy, Applixure will delete all aforementioned Personal Data in its possession within a reasonable timeframe or render it anonymous. Information required for registration to our Services is retained during the subscription term plus 2 months30 days. Other detailed retention times can be provided upon requests.

For what collected information is used

Personal data is used (under the applicable legal basis) to: a) Provide the Services (contract or its preparation, legitimate interest); b) Improve and personalize the Services, as well as to develop new products and services (legitimate interest, consent); c) Correspond with Users regarding customer service issues and support (contract or its preparation, legitimate interest); d) Ensure the functioning and maintenance of the Services (legitimate interest); e) Ensure compliance with the terms applicable to the Services and this Privacy Policy (legitimate interest); and f) Direct marketing based on company's legitimate interest to send you promotional material about products and services you might be interested in. The data subject has the right to refuse personal data being used for direct marketing and may at any time recall prior consent.

For processing activities that are based on a legitimate interest, we have carefully balanced such legitimate interest with the data subjects right to privacy and concluded that our interest outweighs the data subjects' rights and freedoms.

Once information is sent to the Services from Devices, it is being handled by automated processes. These processes divide the uploaded information into two parts, as Personal Data and Non-Personal Data. Depending on the type of Customer Data uploaded, Personal Data are those parts of the said data that directly tie to customer-specific information, such as computer names or usernames. Non-Personal Data is technical information from Devices that are not generally Customer specific, such

as Windows version numbers, application names or are purely statistical information such as length of computer startup time.

Identifiable and Non-Personal Data are stored separately in the Services, so that all Personal Data are always associated with the environment it relates to, and so can be completely removed if Customer decides to end the use of Software and Services.

We use anonymized, statistical and/or aggregate information drawn from environments to compare environments to others using the Services, in order to provide benchmarking functionality. Use of such information will not identify the Customer, Users or any other person individually.

Who has access to the Personal Data

For the purposes stated in this Privacy Policy, the Personal Data may be disclosed, when necessary, to authorities, and to other third parties, such as third-party service providers (such as our hosting providers, IT vendors and marketing agencies conducting marketing on our behalf etc.). In such case, the Personal Data will only be disclosed for purposes defined above. List of the processors and other recipients can be provided upon a request. In addition, Applixure may share the Personal Data in connection with any merger, sale of our assets, or a financing or acquisition of all or a portion of our business and in connection with other similar arrangements. The Personal Data is also disclosed to third parties if required under any applicable law or regulation or order by competent authorities, and to investigate possible infringing use of the products and services as well as to guarantee the safety of the products and services.

Protecting of Data

Applixure takes reasonable measures to protect Personal Data as the data is transferred from end-users' devices to Applixure and to protect the data from loss, misuse, and unauthorized access, disclosure, alteration, and destruction. All Applixure's personnel or subcontractors processing Personal Data are obliged to keep Personal Data strictly confidential.

The Services will be maintained on external service providers' servers with appropriate safeguards. The Services are protected by appropriate industry standard, technical and organizational safety measures, including encryption of data in transit and encryption of data at rest using industry-standard cipher algorithms. Although Applixure makes good faith efforts to store the data collected from the Services in a secure operating environment that is not available to the public, Applixure cannot guarantee the absolute security of that information during its transmission or its storage on our systems. Applixure will post a notice in the Services in case material security breach that endangers privacy or Personal Data, and, will contact affected end-users directly as provided in the applicable data protection legislation. Applixure may also temporarily shut down the Services to protect the Personal Data.

Is data transferred outside the European Union or the European Economic Area

Applixure processes and stores the Personal Data using servers located physically within the European Economic Area (EEA), primarily in Finland. For customers residing outside the EEA, parts of the underlying infrastructure for the Applixure Analytics and Applixure Workflow services are also located in the United Kingdom and the United States to serve their respective geographic areas; no data for a customer environment designated as being in the EU/EEA is processed or stored outside the EU/EEA. Applixure reserves the right to add additional geographic areas to provide Services from other locations following applicable data protection legislation. In case Personal Data is transferred outside EU/EEA, such transfers are either made to a country that is deemed to provide a sufficient level of privacy protection by the European Commission or transfers are carried out by using appropriate safeguards such as standard data protection clauses adopted or otherwise approved by the EU Commission or competent data protection authority in accordance with the GDPR.

Rights of the Data Subjects and Contact Information

Right of access and right of inspection

The data subject has the right to obtain confirmation as to whether or not personal data concerning him or her is being processed. The data subject has the right to inspect and view data concerning him or her and, upon a request, the right to obtain the data in a written or electric form. This applies to information that the data subject has provided to the company insofar the processing is based on a contract/consent. Exercising this right is generally free of charge. Right to rectification and right to erasure The data subject has the right to require us to delete or stop processing the data subject's personal data, for example where the data is no longer necessary for the purposes of processing.

However, please note that certain personal data is strictly necessary in order to achieve the purposes defined in this privacy statement and may also be required to be retained by applicable laws.

Right to data portability

The data subject has the right to receive the personal data that he or she has provided to us in a structured, commonly used and machine-readable format and, if desired, transmit that data to another controller. This right applies when the processing of the personal data is based on consent or a contract. Right to restriction of processing The data subject has the right, under conditions defined by data protection legislation, to request the restriction of processing of his/her personal data. In situations where personal data suspected to be incorrect cannot be corrected or removed, or if the removal request is unclear, the company will limit the access to such data.

Right to object to processing

The data subject has the right to object to the processing of data where we are relying on its legitimate interests as the legal ground for processing. For example, the data subject may object to his/her personal data being used for marketing purposes.

Right to withdraw consent

In cases where the processing is based on the data subjects' consent, he/she has the right to withdraw his/her consent to such processing at any time.

How to use the rights

These rights may be used by sending a letter or e-mail to us on the addresses set out below. We may request the provision of additional information necessary to confirm your identity. We may reject requests that are unreasonably repetitive, excessive or manifestly unfounded. In case you consider our processing activities of Personal Data to be inconsistent with the applicable data protection laws, a complaint may be lodged with the local supervisory authority for data protection.

Right to lodge a complaint with a supervisory authority

The data subject has the right to lodge a complaint with a competent data protection authority if the data subject considers that the processing of personal data relating to him or her infringes current legislation. However, we request that the matter be dealt with Applixure in the first instance. The relevant authority in Finland is the Data Protection Ombudsman (www.tietosuoja.fi).

Changes to the Privacy Policy

We reserve the right to modify this Privacy Policy at any time. If we make changes to this Privacy Policy, we will post a notice in the Services along with the updated Privacy Policy. The data subjects are highly recommended to review the Privacy Policy on our website every now and then. If the data subject objects to any of the changes to this Privacy Policy, the data subject should cease using the Services, where applicable, and he/she can request that we remove the Personal Data, unless applicable laws require us to retain such Personal Data. Unless stated otherwise, the then-current Privacy Policy applies to all Personal Data we process at the time.

Contact info:

Applixure Oy

Business ID: 2507933-3

Address: Arabiankatu 12, 00560 HELSINKI, Finland

Email: info@applixure.com

www.applixure.com