

Zabbix Mobile Application Privacy Policy

Approved: September 15th, 2026

The Zabbix Mobile Application Privacy Policy has been prepared in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (“GDPR”), and other applicable laws and regulations in the area of privacy and data processing.

The Controller responsible for the processing of the personal data described in this Zabbix Mobile Application Privacy Policy is Zabbix SIA, a company registered in the Republic of Latvia under unified registration number 40003738045, registered office: Gustava Zemgala gatve 74, Riga, LV-1039, Latvia.

1. About this Privacy Policy

This Privacy Policy applies exclusively to the Zabbix Mobile Application (the “Application”) and describes the processing of personal data in connection with its use. The Application is used in connection with the Zabbix Monitoring Solution software developed by Zabbix SIA (the “Software”). The Application is intended for business or professional monitoring purposes and may be accessed only by individuals who have been granted access by an authorised administrator to an existing Zabbix Server or Zabbix Cloud user account (a “Software Account”). Users sign in to the Application using the credentials associated with their Software Account. The Application does not create or maintain a separate user account.

The Privacy Policy explains how the Controller processes personal data when you access or use the Application, sign in using an existing Software Account, use the Application’s monitoring functions, contact customer support or otherwise interact with the Controller through or in connection with the Application.

2. Information the Controller Processes

The Controller processes personal data that you provide directly, information generated through your use of the Application, and technical information collected automatically when the Application interacts with the Controller’s systems.

The Application is available only to existing authorised users who have been assigned access credentials for the Software Account.

2.1 Account and Authentication Information

When you sign in to the Application, the Controller may process information associated with your existing Software Account, including your email address, username, user or Software Account identifier, and authentication information. Depending on how your existing Software Account has been configured, your username or email address may or may not include personal data. The information is determined by Software Account administrator, not by the Controller.

Providing Software Account and authentication information is necessary to sign in to and use the Application; without it, the Controller will not be able to authenticate you and you will not be able to access the Application’s functions.

2.2 Customer’s Content

The Application may allow you to view or access data, information or other content already available through the use of Software (“Customer’s Content”).

The Application does not create or retain a separate copy of Customer's Content solely because that content is accessed through the Application. The Controller does not use Customer's Content for purposes unrelated to providing the requested Application functions.

2.3 Technical and Usage Information

When you access or use the Application, the Controller may automatically process technical, device and usage information, including your device manufacturer, model, operating system, unique device or installation identifiers, connection and authentication identifiers, device status, and access and activity dates and times. This information may identify your device or may be associated with your Software Account, device or activity.

When a device is registered for use with the Application, the Controller processes server and device identifiers, client authentication identifiers and credentials, registration status, and information relating to the connection between the registered server and device.

The Controller also processes your IP address, session information, diagnostic information, crash reports, security logs and performance data. Performance data may include response and loading times, failed requests, errors, crashes and other information concerning the technical performance and reliability of the Application.

2.4 Device Permissions

The Application may request access to your device camera and precise location. Access is requested through the device operating system and can be managed through your device settings.

Camera access is used only to scan QR codes. Images are processed locally on the device and are not stored by or transmitted to the Controller.

The Application may request access to your device's location to determine the country from which the Application is used. Location information is accessed only while the Application is in use. Precise location information is processed locally on your device solely to determine the relevant country. The Controller receives only country-level location information and does not receive or store your precise geographic coordinates.

The Application does not require access to your device microphone, contacts, photo library, Bluetooth or other information.

The Application may also allow you to use biometric authentication supported by your device. Biometric verification is performed by the device operating system. The Controller does not receive or store your biometric data and receives only confirmation of whether authentication was successful.

2.5 Feedback and Support Communications

When you submit feedback, report a bug or contact customer support, the Controller processes your email address, the subject and content of your communication, and any documents, screenshots or other materials you choose to provide.

Any feedback or bug report automatically includes technical information about your device and the Application, such as the device manufacturer and model, operating system and API version, security patch date, Application version and build number, and a unique report identifier. This information is included to help the Controller identify, investigate and resolve the reported issue.

Your communication and any materials you provide may contain additional personal data if you choose to include such information. Please avoid including personal data that is not necessary for the handling of your request.

3. Purposes and Legal Bases for Processing

The Controller processes personal data only where there is a valid legal basis and only to the extent necessary for the purposes described below.

3.1 Access to and Operation of the Application

The Controller processes Software Account and authentication information to:

- authenticate existing authorised users;
- provide access to the Application and its functions;
- maintain and administer user access; and
- communicate with users about the operation of the Application.

The Application does not create a separate Software Account. Users access the Application using the credentials associated with their existing Software Account.

This processing is necessary for the performance of the applicable agreement or, where access is provided through an organisation, is based on the Controller's legitimate interest in providing and administering the Application in accordance with that agreement.

3.2 Location Analytics

The Controller processes country-level location information to understand the aggregated geographic distribution of the Application's use to plan infrastructure capacity and improve regional availability and support. This processing is based on your consent, which you indicate by granting the Application permission to access your device's location.

Granting location permission is optional. You may refuse location permission or withdraw your consent at any time through your device settings without affecting your ability to use the Application.

3.3 Security, Maintenance and Technical Performance

The Controller processes technical, device and usage information, including server and device registration information and client authentication identifiers and credentials, to:

- authenticate authorised users and devices;
- administer server and device registrations;
- establish and secure connections between the Application, and the relevant Software infrastructure;
- protect user Software Accounts and prevent unauthorised access;
- maintain the security, availability and technical performance of the Application and related infrastructure;
- identify, diagnose and resolve errors, connection failures and other technical problems; and
- prevent, detect and investigate security incidents or suspected misuse.

This processing is based on the Controller's legitimate interests in operating and maintaining a secure and reliable Application, protecting its systems and users, and preventing unauthorised access or misuse.

3.4 Feedback and Customer Support

The Controller processes the information set out in Section 2.5 to:

- respond to your request or feedback;
- provide technical assistance;
- identify, investigate and resolve reported problems;

- maintain and improve the security and reliability of the Application; and
- investigate suspected misuse of the Application.

This processing is based on the performance of the applicable agreement or the Controller's legitimate interests in providing customer support and maintaining a secure and reliable Application.

3.5 Compliance with Law and Protection of Legal Rights

The Controller may process relevant personal data where necessary to comply with applicable laws, court orders or lawful requests from competent authorities, or to establish, exercise or defend legal claims.

This processing is based on compliance with a legal obligation or the Controller's legitimate interests in protecting and enforcing its legal rights.

4. Account Administration and Personal Data Access, Correction and Deletion

4.1 Accessing and Correcting Personal Data

You may request access to personal data relating to you and request the correction of inaccurate or incomplete personal data.

Where information associated with your Software Account can be corrected or updated by an authorised Software Account administrator, you may submit your request to that administrator. If you are unable to have the information corrected or updated in this way, you may contact the Controller using the contact details provided in this Privacy Policy.

Where the involvement of an Software Account administrator is necessary to implement your request, the Controller may refer the relevant part of the request to that administrator. Only information reasonably necessary to implement the request will be disclosed.

4.2 Account Administration, Offboarding and Deletion Requests

Requests to deactivate, remove or delete a Software Account should be submitted to the relevant Software Account administrator. The administrator may complete the applicable offboarding process, which terminates the Software Account's access to the Application and the relevant Software environment.

You may also contact the Controller using the contact details provided in this Privacy Policy to request the deletion of personal data relating to you. Where the involvement of the authorised Software Account administrator is necessary, the Controller may refer the relevant part of the request to that administrator. Only information reasonably necessary to process the request will be disclosed.

Requests concerning the deletion of personal data will be assessed in accordance with applicable data protection law. Offboarding, deactivation or removal of a Software Account does not necessarily result in the immediate deletion of all personal data associated with the Software Account.

Deleting the Application from your device does not offboard, deactivate or delete your Software Account and does not by itself delete personal data associated with that Software Account.

4.3 Information Retained Following Offboarding or Deletion

Following offboarding, Software Account deactivation or a valid request for the deletion of personal data, the Controller will delete personal data for which continued processing is no longer necessary, subject to the retention periods and exceptions described in this Privacy Policy.

Certain personal data may continue to be retained where and for as long as retention is necessary to:

- comply with applicable legal obligations;
- maintain appropriate security and audit records;
- prevent, detect or investigate security incidents, fraud or suspected misuse;
- resolve disputes; or
- establish, exercise or defend legal claims.

Server and device identifiers, registration records, client authentication information, account or device status information, and relevant security records may therefore be retained for the periods specified in the “Data Retention and Security” section of this Privacy Policy.

4.4 Submitting and Verifying Requests

The Controller may request information reasonably necessary to verify your identity and, where necessary, consult the authorised Software Account administrator to process your request.

5. Data Sharing and International Transfers

5.1 Service Providers and Other Disclosures

The Controller does not sell personal data.

The Controller uses Amazon Web Services (“AWS”) to provide hosting and technical infrastructure for the Application. In providing these services, AWS may process encrypted device identifiers and related technical information on the Controller’s instructions. Access to this information is limited to authorised developers where necessary for the operation, maintenance and security of the Application. AWS processes this information under a data processing agreement incorporating appropriate contractual safeguards.

Where you enable push notifications, the Controller uses mobile platform notification providers (such as Apple Push Notification service and/or Firebase Cloud Messaging) to deliver notifications to your device. These providers process device push tokens and notification metadata to the extent necessary to route notifications, under their respective platform terms and, where applicable, a data processing agreement with the Controller.

The Controller may also disclose personal data to professional advisers, auditors, insurers or public authorities where reasonably necessary or required by law.

5.2 International Data Transfers

The Controller stores and processes personal data relating to the Application within the European Economic Area (“EEA”).

The Controller does not transfer such personal data outside the EEA unless the transfer is necessary and permitted under applicable data protection law. Any such transfer will be protected by an appropriate legal safeguard, such as an adequacy decision, the EU–US Data Privacy Framework where applicable, Standard Contractual Clauses or another lawful transfer mechanism.

6. Data Retention and Security

The Controller retains personal data only for as long as necessary for the purposes described in this Privacy Policy. The applicable retention period depends on the type of information and the purpose for which it is processed.

Software Account information is retained for as long as the user remains authorised by the Software Account administrator to access the Application.

Client authentication credentials are retained for as long as the relevant device registration remains active. Server and device registration records and related security information may be retained thereafter for as long as necessary for security, audit and incident-investigation purposes or to comply with applicable legal obligations.

Diagnostic information, crash reports, security logs and general performance data retained by the Controller do not contain personal data or identifiers that enable the information to be linked to an identifiable individual. As non-personal technical data, this information may be retained without a fixed retention period for system security, diagnostics and performance analysis.

Country-level location information is retained for 90 days from collection, as this period is sufficient to determine in which regions and to what extent the Application is used.

Feedback, bug reports and customer support communications, including related technical information and materials provided by the user, are retained as part of the Controller's email correspondence for as long as necessary to handle and document the relevant matter, including any necessary follow-up, dispute resolution or legal claims.

The Controller may retain particular information for a longer period where necessary to comply with a legal obligation, investigate suspected misuse or a security incident, resolve a dispute, or establish, exercise or defend legal claims. The information will be deleted when its continued retention is no longer necessary.

The Controller protects personal data through appropriate technical and organisational measures, including encryption and access controls.

7. Your Data Protection Rights

Subject to the GDPR and applicable limitations, the following rights to:

- obtain confirmation of whether the Controller processes your data and receive access to it;
- correct inaccurate or incomplete data;
- request deletion of data;
- restrict processing;
- object to processing based on legitimate interests, including related profiling;
- withdraw consent at any time where processing relies on consent, without affecting prior lawful processing;
- lodge a complaint with a supervisory authority.

To exercise your rights, contact the Controller using the contact details provided at the end of this Privacy Policy.

You may lodge a complaint with the Data State Inspectorate of the Republic of Latvia (Datu valsts inspekcija), Elijas iela 17, Riga, LV-1050, Latvia, or with the supervisory authority in the EEA country where you live, work or believe an infringement occurred.

8. Changes to this Policy

The Controller may update this Policy when the Application, our processing or legal requirements change. The Controller will post the updated version at a publicly accessible URL and within the App, identify the effective date and provide additional notice where a change materially affects users or where consent is required.

9. Contact us

Zabbix SIA, Registration No.: 40003738045

Registered Address: Gustava Zemgala gatve 74, Riga, LV-1039, Latvia

Email: legal@zabbix.com

Website: www.zabbix.com