valiantys

Valiantys' GDPR Commitment

Our commitment to your data privacy

We are wholly invested in our customers' success and the protection of customer data. One way that we deliver on this promise is by helping Valiantys customers and users understand, and where applicable, comply with the General Data Protection Regulation (GDPR). The GDPR is the most significant change to European data privacy legislation in the last 20 years and went into effect on May 25, 2018.
It is designed to give EU citizens more control over their data and seeks to unify a number of existing privacy and security laws under one comprehensive law. The GDPR not only applies to organizations located within the EU, but it also applies to all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the company's location.

On this page, we explain our approach and investment in GDPR compliance and how we help our customers comply with the GDPR.

GDPR Compliance

We appreciate that our customers have requirements under the GDPR that are directly impacted by their use of Valiantys and services, which is why we have devoted significant resources toward helping our customers fulfill their requirements under the GDPR and local law.

Below are several GDPR initiatives that have been implemented for our cloud products:

- We have made significant investments in our security infrastructure and certifications (see **Security & Backup Policy**).
- We support appropriate international data transfer mechanisms by executing Standard Contractual Clauses through our updated **Data Processing Agreement**.
- We offer data portability and data management tools including:
    - Profile deletion tools: We help customers and end users delete personal information from Valiantys systems, such as names and email addresses.
        - We help customers **delete their account with Valiantys Support**
        - As well as people without Valiantys Support accounts to **delete their personal information from our systems**
        - But we also help our customers respond to end-user requests to delete personal information from the Atlassian applications we host for customers

        (see Atlassian Product Specific Resources for detailed guides below)
    - Import and export tools: Customers may access, import, and export their Customer Data using Atlassian's tools. See details **here** for Jira and **here** for Confluence.
- We have made required updates to relevant contractual terms.
- We have ensured Valiantys staff that access and process Valiantys customer personal data have been trained in handling that data and are bound to maintain the confidentiality and security of that data.
- We hold any vendors that handle personal data to the same data management, security, and privacy practices and standards to which we hold ourselves.
- We have committed to carrying out data impact assessments and consulting with EU regulators where appropriate.

Our Security and Certifications

Protecting our customers' information and their user's privacy is extremely important to us. We are entrusted with some of our customer's most valuable data, which is why we have built security into every layer of the Valiantys Cloud architecture. We provide replication, backup, and disaster recovery planning, encryption in transit, and more. Visit the **Security & Backup Policy** page to learn more about our approach to security.
Additionally, we have devoted significant resources towards ensuring our cloud services are built and designed in accordance with widely accepted standards and certifications. These standards mirror many of the security and privacy requirements of the GDPR and give our customers a transparent framework by which to measure our software development and data management practices.

Our cloud services are built on the Amazon Web Services infrastructure, which is certified for PCI-DSS Level 1, SOC1, SOC2, SOC3, ISO/IEC 27001, ISO/IEC 9001, and ISO/IEC 27018 standards. To learn more about Amazon Web Services's current certifications and commitments, please see the **Compliance Center** on the AWS website.

International Data Transfers

We offer customers a robust international data transfer framework as a part of our Data Processing Agreement. This agreement ensures that our customers can lawfully transfer personal data to Valiantys outside of the European Economic Area by relying on the Standard Contractual Clauses. This agreement also contains specific provisions to assist customers in their compliance with the GDPR.

Data Portability and the Right to Be Forgotten

We help you honor your customers' requests to export their data, should you host your customer data on Atlassian products hosted for you by Valiantys. Atlassian provides robust data portability and data management tools for exporting product and user data. For more information on Atlassian data export see details **here** for Jira and **here** for Confluence.

We also help customers meet obligations under the GDPR right to be forgotten (or right to erasure) clause by making it easy to delete personal data from Atlassian products.

Valiantys Support can **facilitate the account deletion** of users from our internal systems. We help people without Valiantys Support accounts to **delete their personal information from our systems**. And we help customers respond to end-user requests to delete personal information from the Atlassian applications we host for customers (see Atlassian Product Specific Resources for detailed guides below).

Privacy and Consent

Your privacy is important to us, and so is being transparent about how we collect, use, and share your information. In our **Privacy Policy**, we share what information we collect, how we use and store that data, and how you can access and control your information.

Atlassian Product-Specific Resources

This information is copied from and refers to Atlassian's documentation.
JIRA Core, JIRA Software and JIRA Service Desk Server and Data Center GDPR support guides

We've created this set of support guides to help you with any GDPR-specific obligations that you may have. The guides are designed to identify where personal data may be located within the product, and, where possible, assist with responding to data subject access requests, including in modifying, restricting or deleting data.

Where a workaround involves running SQL scripts directly on your database, we strongly recommend you do this first on a non-production, staging or test environment before running the scripts on your production database. We also strongly recommend you take a backup of your data before making any modifications via SQL scripts.

- **JIRA: Automated individual decision-making, including profiling**
- **JIRA: Communication of personal data breaches**
- **JIRA: Data protection by design and by default**
- **JIRA: Records of processing activities**
- **JIRA: Right of access by the data subject**
- **JIRA: Right to data portability**
- **JIRA: Right to erasure**
- **JIRA: Right to object**
- **JIRA: Right to rectification**
- **JIRA: Right to restriction of processing**
- **JIRA: Security of processing**
- **JIRA: Transfers of personal data to third countries or international organisations**

GDPR support guides for Confluence Server and Data Center

We’ve created this set of support guides to help you with any GDPR-specific obligations that you may have. The guides are designed to identify where personal data may be located within the product, and, where possible, assist with responding to data subject access requests, including in modifying, restricting or deleting data.

Where a workaround involves running SQL scripts directly on your database, we strongly recommend you do this first on a non-production, staging or test environment before running the scripts on your production database. We also strongly recommend you take a backup of your data before making any modifications via SQL scripts.

- Automated individual decision-making, including profiling in Confluence Server and Data Center
- Communication of personal data breaches in Confluence Server and Data Center
- Data Protection by Design and by Default in Confluence Server and Data Center
- Records of processing activities in Confluence Server and Data Center
- Right of access by the data subject in Confluence Server and Data Center
- Right to data portability in Confluence Server and Data Center
- Right to erasure in Confluence Server and Data Center
- Right to object in Confluence Server and Data Center
- Right to rectification in Confluence Server and Data Center
- Right to restriction of processing in Confluence Server and Data Center
- Security of processing in Confluence Server and Data Center
- Transfers of personal data to third countries or international organisations in Confluence Server and Data Center

Bitbucket Server and Data Center GDPR support guides

We’ve created this set of support guides to help you with any GDPR-specific obligations that you may have. The guides are designed to identify where personal data may be located within the product, and, where possible, assist with responding to data subject access requests, including in modifying, restricting or deleting data.

Where a workaround involves running SQL scripts directly on your database, we strongly recommend you do this first on a non-production, staging or test environment before running the scripts on your production database. We also strongly recommend you take a backup of your data before making any modifications via SQL scripts.

- Automated individual decision-making, including profiling in Bitbucket Server and Data Center
- Communication of personal data breaches in Bitbucket Server and Data Center
- Data protection by design and by default in Bitbucket Server and Data Center
- Records of processing activities in Bitbucket Server and Data Center
- Right of access by the data subject in Bitbucket Server and Data Center
- Right to data portability in Bitbucket Server and Data Center

- Right to erasure in Bitbucket Server and Data Center
- Right to object in Bitbucket Server and Data Center
- Right to rectification in Bitbucket Server and Data Center
- Right to restriction of processing in Bitbucket Server and Data Center
- Security of processing in Bitbucket Server and Data Center
- Transfers of personal data to third countries or international organisations in Bitbucket Server and Data Center

Bamboo Server GDPR support guides

We’ve created this set of support guides to help you with any GDPR-specific obligations that you may have. The guides are designed to identify where personal data may be located within the product, and, where possible, assist with responding to data subject access requests, including in modifying, restricting or deleting data.

Where a workaround involves running SQL scripts directly on your database, we strongly recommend you do this first on a non-production, staging or test environment before running the scripts on your production database. We also strongly recommend you take a backup of your data before making any modifications via SQL scripts.

- Bamboo: Automated individual decision-making, including profiling
- Bamboo: Communication of personal data breaches
- Bamboo: Data protection by design and by default
- Bamboo: Records of processing activities
- Bamboo: Right of access by the data subject
- Bamboo: Right to data portability
- Bamboo: Right to erasure
- Bamboo: Right to object
- Bamboo: Right to rectification
- Bamboo: Right to restriction of processing
- Bamboo: Security of processing
- Bamboo: Transfers of personal data to third countries or international organisations

Crowd Server and Data Center GDPR support guides

We’ve created this set of support guides to help you with any GDPR-specific obligations that you may have. The guides are designed to identify where personal data may be located within the product, and, where possible, assist with responding to data subject access requests, including in modifying, restricting or deleting data.

Where a workaround involves running SQL scripts directly on your database, we strongly recommend you do this first on a non-production, staging or test environment before running the scripts on your production database. We also strongly recommend you take a backup of your data before making any modifications via SQL scripts.

- Crowd: Automated individual decision-making, including profiling
- Crowd: Communication of personal data breaches
- Crowd: Data protection by design and by default
- Crowd: Records of processing activities
- Crowd: Right of access by the data subject
- Crowd: Right to data portability
- Crowd: Right to erasure
- Crowd: Right to object
- Crowd: Right to rectification
- Crowd: Right to restriction of processing
- Crowd: Security of processing
- Crowd: Transfers of personal data to third countries or international organisations

Fisheye and Crucible Server GDPR support guides

We've created this set of support guides to help you with any GDPR-specific obligations that you may have. The guides are designed to identify where personal data may be located within the product, and, where possible, assist with responding to data subject access requests, including in modifying, restricting or deleting data.

Where a workaround involves running SQL scripts directly on your database, we strongly recommend you do this first on a non-production, staging or test environment before running the scripts on your production database. We also strongly recommend you take a backup of your data before making any modifications via SQL scripts.

- Fisheye and Crucible: Automated individual decision-making, including profiling
- Fisheye and Crucible: Communication of personal data breaches
- Fisheye and Crucible: Data protection by design and by default
- Fisheye and Crucible: Records of processing activities
- Fisheye and Crucible: Right of access by the data subject
- Fisheye and Crucible: Right to data portability
- Fisheye and Crucible: Right to erasure
- Fisheye and Crucible: Right to object
- Fisheye and Crucible: Right to rectification
- Fisheye and Crucible: Right to restriction of processing
- Fisheye and Crucible: Security of processing
- Fisheye and Crucible: Transfers of personal data to third countries or international organisations

Portfolio for Jira Server GDPR support guides

We've created this set of support guides to help you with any GDPR-specific obligations that you may have. The guides are designed to identify where personal data may be located within the product, and, where possible, assist with responding to data subject access requests, including in modifying, restricting or deleting data.

Where a workaround involves running SQL scripts directly on your database, we strongly recommend you do this first on a non-production, staging or test environment before running the scripts on your production database. We also strongly recommend you take a backup of your data before making any modifications via SQL scripts.

- **Right to erasure in Portfolio for Jira Server and Data Center**
- **Right to rectification in Portfolio for Jira Server and Data Center**

GDPR and Atlassian Cloud applications

Using an Atlassian Cloud application? Head to **www.atlassian.com/trust/privacy/gdpr** for more information.