Standard Contractual Clauses

SECTION I

Clause 1

Purpose and scope

a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of 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.

b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29 (3) and (4) Regulation (EU) 2018/1725.

c) These Clauses apply to the processing of personal data as specified in Annex II.

d) Annexes I to IV are an integral part of the Clauses.

e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2

Invariability of the Clauses

a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3

Interpretation

a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5 – Optional

Docking clause

a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION II

OBLIGATIONS OF THE PARTIES

Clause 6

Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause 7

Obligations of the Parties

7.1 Instructions

a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2 Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3 Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4 Security of processing

a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5 Sensitive Data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6 Documentation und compliance

a) The Parties shall be able to demonstrate compliance with these Clauses.

b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7 Use of sub-processors

a) The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 14 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that

the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8 International transfers

a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8

Assistance to the controller

a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

   i) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

   ii) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

   iii) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

   iv) the obligations in Article 32 Regulation (EU) 2016/679.

d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9

Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679 or under Articles 34 and 35 Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

b) in obtaining the following information which, pursuant to Article 33(3) Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:

   i) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

   ii) the likely consequences of the personal data breach;

iii) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

c) in complying, pursuant to Article 34 Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

b) the details of a contact point where more information concerning the personal data breach can be obtained;

c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III

FINAL PROVISIONS

Clause 10

Non-compliance with the Clauses and termination

a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

   i) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

   ii) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

   iii) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I

LIST OF PARTIES

Controller:

Name	
Adress	
Contact person's name, position and contact details	
Contact details of the data protection officer	

Signature and accession date:

Processor:

Name	Communardo Products GmbH
Adress	Kleiststr. 10a, 01129 Dresden, Germany
Contact details of the data protection officer	DID Dresden Institute for Data Protection +49 (0)351 655 772-0 datenschutz@communardo.de

Signature and accession date: Dresden, 10. July 2025

ANNEX II

DESCRIPTION OF THE PROCESSING

General processing information

This table provides general information about data processing practices applicable to all our self-hosted Atlassian Cloud apps.

The app-specific tables that follow build upon this baseline by adding or refining details - such as the specific types of data processed, processing purposes, and categories of data subjects relevant to each app.

Categories of affected persons	Users of the data controller's Confluence,Jira Cloud, including employees, contractors and customers.
Categories of personal data	All listed Cloud apps process the following personal data. Additional data is maybe listed in the following app specific tables • IP address • User agent • Event tracking
Type of processing	The nature of the processing results from the description of the application and includes in particular the automated collection, transmission and storage of personal data to ensure the functionality of the application.
Purpose of the processing	**IP address, user agent** This is used to select the best CDN location for the AWS or Azure content delivery network as well for routing your request through the infrastructure **Event tracking** We track certain in-app events to ensure our app works reliably and continues to improve based on real usage. This includes understanding which features are used, identifying issues early, and ensuring secure and compliant operation. Event tracking helps us deliver a better, more tailored user experience - while respecting data minimization and privacy principles **Atlassian AccountId (Some apps)** The Atlassian accountId is a unique identifier assigned by Atlassian to each user in the Atlassian Cloud. It is used by some of our apps to manage user-specific data, such as activity logs or role assignments. Important note: We only store or process this accountId in some apps. If an app explicitly uses or stores the Atlassian accountId, it will be listed in the app-specific table within this SCC documentation, along with details of how and why it is processed.
Duration of processing	The processing of personal data takes place for the duration of the use of the application. Processing of personal data stored in log files may take place for up to 90 days after termination of use. The browser local storage is cleared on user logout, the browser session storage is cleared on window or tab close.
Sub-processors	All our apps use as sub-processors:

	Atlassian Pty Ltd, Communardo Software sh.p.k, Communardo Switzerland AG, Mibex Software GmbH (Member of the Communardo Group) Additional ones are listed in the specific app tables

SharePoint Connector for Confluence Cloud

Description	With the Confluence app you can combine Confluence's free-form, easy to edit wiki with the document management of SharePoint Online. The SharePoint WebPart easily embed Confluence pages in SharePoint.
Categories of affected persons	Nothing additional
Categories of personal data	• Meta data (for example document or list id, descriptions and settings) • Access token (Confluence App)
Processed sensitive data	None
Type of processing	Nothing additional
Purpose of the processing	The purpose of the processing of personal data includes the provision of the application using the Microsoft Azure content delivery network, Microsoft Graph API (Confluence App) and the Confluence API (SharePoint WebPart) . The processing of personal data is necessary for the provision of the application. The browser local storage and the browser session storage are used to ensure authentication. The processor does not have access to the controller's content data processed within the Confluence Cloud or SharePoint at any time.
Duration of processing	Nothing additional
Sub-processors	Microsoft Ireland Operations Ltd

SharePoint Connector for Jira Cloud

Description	View connected SharePoint documents or files in Jira with the Jira app. It includes file filtering options and search. The SharePoint WebPart allows to connect and display Jira issues in SharePoint pages.
Categories of affected persons	Nothing additional
Categories of personal data	• Meta data (for example document or list id, descriptions and settings) • User Avatar (Jira App) • Session token (Jira App) • Authentication state (SharePoint WebPart) • Access token (SharePoint WebPart)
Processed sensitive data	None
Type of processing	Nothing additional
Purpose of the processing	The purpose of the processing of personal data includes the provision of the application using Atlassian Forge, Microsoft Graph API (Jira App) and the provision of the application using Microsoft Azure (SharePoint WebPart) . The processing of personal data is necessary for the provision of the application. The user avatars are processed to minimize the network traffic and increase performance to load the same user avatars multiple times (optional). The session token, authentication state and access token are used to ensure authentication. The processor does not have access to the controller's content data processed within the Jira Cloud or SharePoint at any time.
Duration of processing	Nothing additional
Sub-processors	Microsoft Ireland Operations Ltd

Metadata for Confluence Cloud

Description	Metadata for Confluence Cloud allows you to centrally assign and administer page metadata in Confluence Cloud. With our Metadata app you can assign content categories to pages, add content categories to Confluence page templates and search metadata and display pages based on their metadata values.
Categories of affected persons	Nothing additional
Categories of personal data	• Atlassian AccountId
Processed sensitive data	None
Type of processing	Nothing additional
Purpose of the processing	The purpose of the processing of personal data includes the provision of the application using the Microsoft Azure content delivery network. The processing of personal data is necessary for the provision of the application. The processor does not have access to the controller's content data processed within the Confluence Cloud at any time.
Duration of processing	Nothing additional
Sub-processors	Microsoft Ireland Operations Ltd

Subspace Navigation Confluence Cloud

Description	SubSpace Navigation offers a simple way organize and navigate Confluence.
Categories of affected persons	Nothing additional
Categories of personal data	Nothing additional
Processed sensitive data	None
Type of processing	Nothing additional
Purpose of the processing	The purpose of the processing of personal data includes the provision of the application using the Microsoft Azure content delivery network. The processing of personal data is necessary for the provision of the application. The browser cache and session storage is used to improve the performance of the application. The processor does not have access to the controller's content data processed within the Confluence Cloud at any time.
Duration of processing	Nothing additional
Sub-processors	Microsoft Ireland Operations Ltd

User Profiles for Confluence Cloud

Description	User Profiles for Confluence allows to display user information from Microsoft 365 on Confluence pages.
Categories of affected persons	Nothing additional
Categories of personal data	• Information from Active Directory, for example name and email address • Authentication characteristics • Atlassian AccountId
Processed sensitive data	None
Type of processing	Nothing additional
Purpose of the processing	The purpose of the processing of personal data includes the provision of the application using the Microsoft Azure content delivery network. The processing of personal data is necessary for the provision of the application. The local storage of the clients is used to ensure authentication. The processor does not have access to the controller's content data processed within the Confluence Cloud at any time.
Duration of processing	Nothing additional
Sub-processors	Microsoft Ireland Operations Ltd

User Profiles for Jira Cloud

Description	User Profiles for Jira allows you to synchronize and display user information from Microsoft 365 on Jira issues.
Categories of affected persons	Nothing additional
Categories of personal data	• Information from Active Directory, for example name and email address • Authentication characteristics • Atlassian AccountId
Processed sensitive data	None
Type of processing	Nothing additional
Purpose of the processing	The purpose of the processing of personal data includes the provision of the application using the Microsoft Azure content delivery network. Furthermore, a download of the information from the Active Directory of the controller takes place. The processor transfers this information to the Jira Cloud of the controller. The processing of personal data is necessary for the provision of the application. The local storage of the clients is used to ensure authentication.
Duration of processing	Nothing additional
Sub-processors	Microsoft Ireland Operations Ltd

Out of Office Sync for Jira and Microsoft

Description	Out of Office Sync for Jira and Microsoft allows to quickly identify unavailable team members in Jira when assigning tasks, ensuring smoother task management
Categories of affected persons	Nothing additional
Categories of personal data	• Information from Active Directory, for example name and email address • Authentication characteristics • Atlassian AccountId
Processed sensitive data	None
Type of processing	Nothing additional
Purpose of the processing	The purpose of the processing of personal data includes the provision of the application using the Microsoft Azure content delivery network. Furthermore, a download of the information from the Active Directory of the controller takes place. The processor transfers this information to the Jira Cloud of the controller. The processing of personal data is necessary for the provision of the application. The local storage of the clients is used to ensure authentication.
Duration of processing	Nothing additional
Sub-processors	Microsoft Ireland Operations Ltd

Navitabs – Navigation Macros for Confluence Cloud

Description	Work with tabs on Confluence pages. Display content from other pages as tabs or create tabs to structure your content
Categories of affected persons	Nothing additional
Categories of personal data	Nothing additional
Processed sensitive data	None
Type of processing	Nothing additional
Purpose of the processing	Nothing additional
Duration of processing	Nothing additional
Sub-processors	Amazon Web Services EMEA, Google Ireland Limited, Sentry

Viewtracker - Analytics for Confluence Cloud

Description	Get Confluence page view insights, track user activity & generate user engagement analytics reports with strong data privacy focus
Categories of affected persons	Nothing additional
Categories of personal data	• Atlassian AccountId • User's full name (Optional) The export of the user's full names is disabled by default and can only be activated by a Confluence Administrator from the Customer (Controller)
Processed sensitive data	None
Type of processing	Nothing additional
Purpose of the processing	**Atlassian AccountId** Usage of the accountId: • Optimize the in-app notification for app updates, to show only new entries to the end user. Depending on the In-App configured privacy mode, we use and/or store the accountId in different ways. *Standard mode* As an analytics app the accountId is stored in the matter who viewed created, deleted and updated content and spaces. *Extended privacy mode* The app doesn't store anymore who viewed created, deleted and updated content and spaces. This very restrictive setting influences a lot of reports, as the app doesn't know who performed those actions. **Content title, Space name** These 2 entities are stored to be able to: • Sort reports by name & title • Filter reports by the space name or content title • To add the Space name and content title to exports and REST APIs we offer our end users. **User's full name** If the option to export the names of content visitors, contributors, and engaged users is activated in the Viewtracker settings, and the user opts to use this feature during the export process, the complete names of the users will be processed and included in the CSV file. This file will be securely stored on the app's infrastructure and available for download for 48 hours before it is automatically deleted. This functionality is disabled by default and can only be activated by a Confluence Administrator from the Customer (Controller), not by Communardo.
Duration of processing	Nothing additional

Sub-processors	Amazon Web Services EMEA, Google Ireland Limited, Sentry

Advanced Panelboxes for Confluence Cloud

Description	Create a set of designed panel boxes to display identical topics in the same style, keeping your pages clear and easy to read
Categories of affected persons	Nothing additional
Categories of personal data	Nothing additional
Processed sensitive data	None
Type of processing	Nothing additional
Purpose of the processing	Nothing additional
Duration of processing	Nothing additional
Sub-processors	Amazon Web Services EMEA, Google Ireland Limited, Sentry

Translations for Confluence Cloud

Description	Display the same content in different languages on a single Confluence page
Categories of affected persons	Users of the data controller's Confluence Cloud, including employees, contractors and customers.
Categories of personal data	Nothing additional
Processed sensitive data	None
Type of processing	Nothing additional
Purpose of the processing	Nothing additional
Duration of processing	Nothing additional
Sub-processors	Amazon Web Services EMEA, Google Ireland Limited, Sentry

Include from Bitbucket to Confluence (Cloud)

Description	Include Git files, pull requests & other data from public or private Bitbucket repositories.
Categories of affected persons	Nothing additional
Categories of personal data	• Atlassian accountId • Bitbucket Authentication token (optional)
Processed sensitive data	None
Type of processing	Nothing additional
Purpose of the processing	**Usage of the Atlassian accountId:** To link authentication token to Atlassian user account **Bitbucket Authentication token** Used to access private repositories.
Duration of processing	Nothing additional
Sub-processors	SFDC Ireland Limited, Better Stack Inc.

Include from GitHub to Confluence (Cloud)

Description	Include Git files, pull requests & other data from public or private GitHub repositories.
Categories of affected persons	Nothing additional
Categories of personal data	• Atlassian accountId • GitHub Authentication token (optional)
Processed sensitive data	None
Type of processing	Nothing additional
Purpose of the processing	**Usage of the Atlassian accountId:** To link authentication token to Atlassian user account **GitHub Authentication token** Used to access private repositories.
Duration of processing	Nothing additional
Sub-processors	SFDC Ireland Limited, Better Stack Inc.

Include from GitLab to Confluence (Cloud)

Description	Include Git files, pull requests & other data from public or private GitLab repositories.
Categories of affected persons	Nothing additional
Categories of personal data	• Atlassian accountId • GitLabAuthentication token (optional)
Processed sensitive data	None
Type of processing	Nothing additional
Purpose of the processing	**Usage of the Atlassian accountId:** To link authentication token to Atlassian user account **GitLabAuthentication token** Used to access private repositories.
Duration of processing	Nothing additional
Sub-processors	SFDC Ireland Limited, Better Stack Inc.

Jupyter Viewer for Confluence (Cloud)

Description	Render Jupyter/IPython notebooks inside Confluence pages.
Categories of affected persons	Nothing additional
Categories of personal data	• Atlassian accountId • GitHub Authentication token (optional)
Processed sensitive data	None
Type of processing	Nothing additional
Purpose of the processing	**Usage of the Atlassian accountId:** To link authentication token to Atlassian user account **GitHub Authentication token** Used to access private repositories.
Duration of processing	Nothing additional
Sub-processors	SFDC Ireland Limited, Better Stack Inc.

Beautiful Math for Confluence (Cloud)

Description	Add beautiful math expressions into Confluence pages by using LaTeX, AsciiMath or MathML.
Categories of affected persons	Nothing additional
Categories of personal data	Nothing additional
Processed sensitive data	None
Type of processing	Nothing additional
Purpose of the processing	Nothing additional
Duration of processing	Nothing additional
Sub-processors	SFDC Ireland Limited, Better Stack Inc.

Include Code Quality for Bitbucket (Cloud)

Description	Shows Sonar statistics for public Bitbucket repositories from public SonarQube servers or SonarCloud.
Categories of affected persons	Nothing additional
Categories of personal data	Nothing additional
Processed sensitive data	None
Type of processing	Nothing additional
Purpose of the processing	Nothing additional
Duration of processing	Nothing additional
Sub-processors	SFDC Ireland Limited, Better Stack Inc.

Code Owners for Bitbucket (Cloud)

Description	Adds Code Owners as reviewers to new pull requests.
Categories of affected persons	Nothing additional
Categories of personal data	Nothing additional
Processed sensitive data	None
Type of processing	Nothing additional
Purpose of the processing	Nothing additional
Duration of processing	Nothing additional
Sub-processors	SFDC Ireland Limited, Better Stack Inc.

DevSensei Auto Merge for Bitbucket (Cloud)

Description	Automatically merge pull requests when ready.
Categories of affected persons	Nothing additional
Categories of personal data	Nothing additional
Processed sensitive data	None
Type of processing	Nothing additional
Purpose of the processing	Nothing additional
Duration of processing	Nothing additional
Sub-processors	SFDC Ireland Limited, Better Stack Inc.

ANNEX III

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Physical access control

Unauthorised persons will be denied access to data processing systems with which personal data is processed or used.

☒ Room use concept

☒ Burglary protection (e.g. security glazing, motion detectors, alarm system, security service)

☒ Access protection (e.g. security locks, chip card/transponder locking system, key regulation)

☒ Manual access control (e.g. personal control by reception, logging of visitors)

☒ Automatic access control system for critical areas

☒ Careful selection of cleaning and security personnel

☒ Organizational requirements for location-independent working

Access control

Unauthorised persons are prevented from using data processing systems.

☒ Central user management (e.g. central user accounts, central access assignment, central device management)

☒ Secure authentication (e.g. password policy, multi-factor authentication)

☒ Automatic locking of devices when inactive

☒ Use of intrusion detection systems (e.g. anti-virus software, intrusion detection system)

☒ Using VPN Connections for Critical Systems

☒ Patch management for OS and applications

Permission control

Guarantee that those authorised to use a data processing system can only access the data subject to their access authorisation and that personal data cannot be read, copied, changed or removed without authorisation during processing, use and after storage.

☒ Authorization concept

☒ Tiered assignment of user rights

☒ Separation of administrative access

☒ Limited number of administrators

☒ Logging of accesses

☒ Data flow control (e.g. software firewall, hardware firewall, functional restrictions)

☒ Encrypted storage on mobile devices / mobile data carriers

☒ Secure deletion of data carriers before reuse

☒ Safe disposal of data carriers (e.g. via certified waste management company, physical destruction, secure deletion)

☒ Safe disposal of paper documents (e.g. via certified waste disposal company, suitable document shredders)

Transfer control

Ensuring that personal data cannot be read, copied, altered or removed without authorisation during electronic transmission or during transport or storage on data carriers, as well as that it is possible to check and determine to which points the transfer of personal data by means of data transmission is envisaged.

☒ Determination of possible recipients of processing

☒ Careful selection of transmission channels

☒ Encrypted, digital transport path (e.g. https, TLS)

☒ Disclosure in anonymised/pseudonymised form

☒ Additional protective measures in the event of claims by controllers
(e.g. email encryption, use of VPN connections)

Input control

Guarantee that it can be checked and determined afterwards whether and by whom personal data has been entered, changed or removed into data processing systems.

☒ Logging of changes to data (e.g. via document management, log files)

☒ Defined responsibilities for deletions

Order control

Ensuring that personal data processed on behalf of the client can only be processed in accordance with the instructions of the client, as well as measures in the event of outsourcing data processing to processors.

☒ Regular awareness raising among employees

☒ Commitment to confidentiality

☒ Data protection processes (e.g. response to data breaches, assertion of data subject rights)

☒ Careful selection of processors

☒ Conclusion of order processing agreements

☒ Regular review of technical and organizational measures (e.g. as part of the audit of the management system according to ISO 27001, through data protection audits, through TOM audits)

Availability check

Ensuring that personal data is protected against accidental destruction or loss.

☒ Use of firewalls

☒ Hazard detection (e.g. by fire and smoke alarm systems, water detectors)

☒ Data backup (e.g. backup in separate fire compartment, external backup)

☒ Redundancies (e.g. mirrored hard disks / system / clusters, external disaster recovery)

☒ Interference safety (e.g. uninterruptible power supply, surge protection, fall-back internet line)

☒ Recovery (e.g. regulation of responsibilities and processes, regular recovery tests, hardware service contracts)

Separation requirement

Ensuring that data collected for different purposes can be processed separately.

☒ Client separation (e.g. by physical or software separation)

☒ Pseudo-/anonymization of test and statistical data

☒ Separation of production and test systems

ANNEX IV

List of sub-processors

The controller has authorized the use of the following sub-processors:

Name	Atlassian Pty Ltd
Adress	Level 6, 341 George Street, Sydney NSW 2000, Australia
Contact person	Mrs. Kelly Gertridge, dataprotection@atlassian.com
Purpose	Providing infrastructure for processing and storing data

Name	Communardo Software sh.p.k
Adress	Rruga Andon Zako Çajupi Nd. 3, H. 16, Tirana 1019, Albania
Contact person	Elison Ramovi - Head of Location Tirana, elison.ramovi@communardo.de
Purpose	Providing Support for the Services

Name	Communardo Switzerland AG
Adress	Hardturmstrasse 101 8005 Zurich, Switzerland
Contact person	Martin Wulff, dataprivacy@communardo.ch
Purpose	Providing Support for the Services

Name	Mibex Software GmbH (Member of the Communardo Group)
Adress	Albisriederstrasse 253, Zurich - 8047, Switzerland, Switzerland
Contact person	Michael Rüegg, dataprivacy@communardo.ch
Purpose	Providing Support for the Services

Name	Microsoft Ireland Operations Ltd
Adress	South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland
Contact person	Microsoft Ireland Operations Limited, Attn: Data Protection Officer Telephone: +353 1 706 3117
Purpose	Providing infrastructure for processing data

Name	Amazon Web Services EMEA
Adress	Avenue John F. Kennedy 38, LUXEMBOURG, 1855, LUXEMBOURG
Purpose	• Providing infrastructure for processing data

Name	Google Ireland Limited
Adress	Gordon House, Barrow Street, Dublin 4, Ireland
Purpose	• anonymized google analytics (can be deactivated on customers request)

Name	Sentry (Sentry is a registered trademark of Functional Software, Inc.)
Adress	45 Fremont Street, 8th Floor, San Francisco, CA 94105
Purpose	• providing the infrastructure for real-time error tracking of our Cloud apps • The privacy statement can be found here

Name	SFDC Ireland Limited
Adress	Salesforce Tower Dublin, North Dock, Dublin 1, D01 W2Y3, Ireland + 353 14403500, legal@salesforce.com
Purpose	Hosting (Heroku) • The provider is using further sub-processors as per the following list https://www.salesforce.com/company/legal/trust-and-compliance-documentation/ • Technical and organizational measures can be found here: https://www.salesforce.com/company/legal/trust-and-compliance-documentation/

Name	Better Stack Inc.
Adress	651 N. Broad Street, Suite 206, Middletown, DE 19709, United States +1 (628) 900-3830, hello@betterstack.com
Purpose	Logging (Heroku)