ATLASSIAN

BaFin Guidelines

Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)'s guidelines on outsourcing arrangements

LAST UPDATED DEC 2021

This chart is designed to help financial services institutions under the supervision of BaFin, the German Federal Financial Supervisory Authority, map how each paragraph in Chapter V (Contractual terms in the case of (material) outsourcing) of the Guidance on Outsourcing to Cloud Service Providers (the "BaFin Guidance") corresponds to Atlassian's customer contract documentation.

If you have an existing Atlassian contract or would like to learn more about how these terms could apply to your contract, please contact us.

	Consideration	Atlassian Commentary
1.	Depending on the supervisory law requirements, the following terms and conditions in particular should be included in the outsourcing agreement for material outsourcing1 or for non-differentiated outsourcing according to the KAGB:	
2.	**1. Scope of performance**	
3	The agreement should include a specification, and if necessary a description, of the service to be performed by the cloud service provider. This should be stipulated in what is referred to as the service level agreement. In this context, the following aspects should be defined:	

	Consideration	Atlassian Commentary
4.	• the item to be outsourced and its implementation (e.g. type of service and deployment model, scope of services offered such as computing power or available memory space, availability requirements, response times),	Our **Documentation**, which is incorporated by reference into the Atlassian customer contract for qualifying customers, contains clear descriptions of the Covered Cloud Products.
5.	• support services	Qualifying customers have access to the **Atlassian Support Offering**, which is subject to the Atlassian customer contract.
6.	• responsibilities, duties of cooperation and provision (e.g. in the case of updates),	Generally addressed by the Atlassian customer contract.
7.	• place of performance (e.g. location of data centres),	Certain Covered Cloud Products include in-product data residency functionality, as further described **here**, which allows our customers' administrators to pin in-scope product data to a location of their choice. **This page** describes our cloud hosting infrastructure. We contractually commit to (a) not materially degrading product functionality during the applicable subscription term, and (b) notifying customers of any changes to our data hosting locations.
8.	• commencement and end of outsourcing agreement,	The Atlassian customer contract sets out the default length of a subscription term and all applicable notice periods. In addition, when you place an order for one or more Covered Cloud Products, it will contain the start and end date of your corresponding subscription term.
9.	• key ratios for performing ongoing review of service level,	The corresponding service level terms, as well as the remedies for not meeting service levels, for the Covered Cloud Products are provided for in our **Service Level Agreement** and the corresponding **Product Specific Terms**.
10.	• indicators for identifying an unacceptable service level.	We publish service availability updates at **https://status.atlassian.com/**, and contractually commit to notifying customers of events that have a material impact on the availability of the Covered Cloud Products.

	Consideration	Atlassian Commentary
11.	**2. Information and audit rights of supervised company**	
12.	Information and audit rights as well as control possibilities of the supervised company must not be subject to contractual restrictions. It has to be ensured that the supervised company receives the information it needs to adequately control and monitor the risks associated with the outsourcing.	Our audit program is designed to allow qualifying customers and their supervisory authorities to audit the Covered Cloud Products effectively.
13.	To safeguard the information and audit rights, the following terms in particular should be contractually agreed: • grant of full access to information and data as well as access to the cloud service provider's business premises, including all data centres, equipment, systems, networks used for providing the items outsourced; this includes the related processes and controls, • effective possibilities of controlling and auditing the entire outsourcing chain.	See row 12, above.
14.	No (indirect) restriction of rightsEffective exercise of the information and audit rights may not be restricted by contract. The German supervisory authorities consider such impermissible restriction of information and auditing rights to exist particularly in the case of contractual agreements granting such rights only subject to certain conditions. This particularly includes: • agreeing on incremental information and audit procedures, e.g. the obligation to first rely on the audit reports, certificates or other proof of compliance with recognised standards by the cloud service provider before the supervised company can perform its own auditing activities, • restricting performance of information and audit rights to submission of audit reports, certificates or other proof of compliance with recognised standards by the cloud service provider, • linking information access to prior attendance of special training programmes, • wording a clause in such a way that performance of an audit is made conditional on its commercial reasonableness, *Continued on next page*	See row 12, above.

	Consideration	Atlassian Commentary
14.	*Continued from previous page* • limiting the performance of audits in terms of timing and personnel; as a general rule, however, it is acceptable to limit access to customary business hours upon advance notice, • making reference to exclusive use e.g. of management consoles for exercising information and audit rights of the company,	See row 12, above.
15.	**Exemptions** Depending on the applicable requirements under supervisory law, the supervised companies may claim exemptions to make their own audit activities more efficient. Such exemptions are pooled audits or the use of documentation/ certificates based on common standards or of audit reports of recognised third parties or of internal audit reports of the cloud service provider.	This is a customer consideration. Please also see row 12, above, and row 20, below.
16.	**Pooled Audits** Supervised companies subject to compliance with sections 25a, 25b KWG may avail themselves of exemptions in Circular 09/2017 (BA) – Minimum Requirements for Risk Management – (MaRisk). Pursuant to BT 2.1 Item 3 MaRisk, the internal auditing function of the supervised company in the case of material outsourcing may forego own auditing activities provided that the auditing work carried out by the external service provider meets the requirements of AT 4.4 and BT 2 MaRisk. The internal auditing function of the supervised outsourcing company must satisfy itself at regular intervals that these conditions are met. The audit findings concerning the supervised company are to be passed on to the internal auditing function of the supervised outsourcing company.	This is a customer consideration. Please also see row 12, above.
17.	In this regard the auditing activity may be performed by the internal audit department of the cloud service provider, the internal audit department of one or more of the supervised outsourcing companies on behalf of the supervised outsourcing companies (“pooled audits”), a third party appointed by the cloud service provider or a third party appointed by the supervised outsourcing companies.	This is a customer consideration. Please also see row 12, above.

	Consideration	Atlassian Commentary
18.	For the other supervised companies, it may be permissible in the individual case to exercise certain information and audit rights against the cloud service provider jointly with other supervised companies by way of pooled audit.	This is a customer consideration. Please also see row 12, above.
19.	If a supervised company avails itself of one of the aforementioned exemptions, this may not result in its information and audit rights being restricted.	See row 12, above.
20.	**Proof/certificates and audit reports** The supervised company as a general rule may use documentation/certificates on the basis of common standards (e.g. international security standard ISO/IEC 2700X of the International Organization for Standardization, Cloud Computing Compliance Controls Catalogue (C 5 Catalogue) of the BSI), audit reports of recognised third parties or internal audit reports of the cloud service provider. The supervised company in this regard must take account of the scope, depth of detail, up-to-dateness and suitability of the certifier or auditor of such documentation/ certificates and audit reports.	Atlassian regularly undergoes independent examination of our security, privacy and compliance controls. During the term of our contract with you, we will comply with at least the standards listed on our Trust Center, which includes ISO/IEC 27001 and ISO/IEC 27018 certifications, and SOC 2 Type II and SOC 3 audit reports: **https://www.atlassian.com/trust/compliance**
21.	However, a supervised company must not rely solely on these when exercising its audit activity. Where the internal audit department uses such documentation/certificates in its activity, it should be able to examine the evidence underlying them.	This is a customer consideration. Please also see row 12, above.
22.	**3. Information and audit rights of supervisory authorities**	
23.	Information and audit rights as well as control possibilities of the supervisory authorities must not be subject to contractual restrictions. The supervisory authorities must be able to monitor cloud service providers exactly as the applicable law provides for the supervised company. It must be possible for the supervisory authorities to exercise their information and audit rights as well as control possibilities properly, and without restriction, as regards the item being outsourced; this also applies to those persons whom the supervisory authorities use when performing the audits.	Our audit program is designed to allow qualifying customers and their supervisory authorities to audit the Covered Cloud Products effectively.

	Consideration	Atlassian Commentary
24.	To safeguard these rights, the following terms in particular should be contractually agreed: • obligation of the cloud service provider to cooperate with the supervisory authorities without restriction, • grant of full access to information and data as well as access to the cloud service provider's business premises, including all data centres, equipment, systems, networks used for providing the items outsourced; this includes the processes and controls relating thereto as well as the possibility of performing on-site audits of the cloud service provider (and where applicable of the chain-outsourcing company), • effective possibilities of controlling and auditing the entire outsourcing chain.	See row 23, above.
25.	**No (indirect) restriction of rights** Such impermissible restriction of information and auditing rights as well as control possibilities of the German supervisory authorities is deemed to exist particularly in the case of provisions granting such rights only on certain conditions. We refer to the above statements on the restriction of the rights of the supervised companies to avoid repetition.	See row 23, above.
26.	**4. Rights to issue instructions**	
27.	Rights of the supervised companies to issue instructions are to be agreed. The rights to issue instructions are to ensure that all required instructions needed to perform the agreed service can be issued, i.e. the possibility of influencing and controlling the outsourced item is required. The technical implementation may be organised individually based on the company's specific circumstances.	Our customers may issue instructions (including with respect to third party certifications and audit reports) to us regarding the Covered Cloud Products through their customer support channels.

	Consideration	Atlassian Commentary
28.	If the supervised company uses proof/ certifications or audit reports (cf. V.2), it should also have the possibility of influencing the scope of proof/certifications or audit reports so that it can be expanded to include relevant systems and controls. There should be a reasonable proportion in how many and how often such instructions are issued.	See row 27, above.
29.	Moreover, the supervised company should be authorised at all times to issue instructions to the cloud service provider for correction, deletion and blocking of data and the cloud service provider should be allowed to collect, process and use the data only in the context of the instructions issued by the supervised company. This should also cover the possibility of issuing an instruction at any time to have the data processed by the cloud service provider transferred back to the supervised company promptly and without restriction.	We offer a **Data Processing Addendum** that provides detailed commitments regarding the processing and security of customer personal data. You can learn more about our GDPR compliance program here: **https://www.atlassian.com/trust/compliance/resources/gdpr** In addition, we provide all customers with in-product functionality to export their data at any time during the term of their contract without our assistance.
30.	If the explicit agreement on the rights of the supervised company to issue instructions can be waived, the service to be provided by the outsourcing company is to be specified with sufficient clarity in the outsourcing agreement.	See row 27, above.
31.	**5. Data security/protection (reference to location of data storage)**	
32.	Provisions ensuring compliance with data protection regulations and other security requirements are to be agreed.	Given the one-to-many nature of our Covered Cloud Products, we provide the same robust security for all of our customers. These security practices are described in detail on our Trust Center: **https://www.atlassian.com/trust/** We commit to complying with the security practices on our Trust Center, and to not materially decreasing the overall security of our Covered Cloud Products during your subscription term. Please also see rows 27 and 29, above.

	Consideration	Atlassian Commentary
33.	The location of data storage must be known to the supervised company. This should include the specific location of the data centres. As a general rule, giving the name of the location (e.g. the town or city) will suffice for this purpose. However, if the supervised company should need the precise address of the data centre based on considerations of risk management, the cloud service provider should provide it.	See row 7, above.
34.	Moreover, redundancy of the data and systems should be ensured so that in the event of a failure of one data centre it is ensured that the services are maintained.	We maintain business continuity plans and disaster recovery plans, as **described on our Trust Center**. These plans are reviewed and tested at least annually.
35.	The security of the data and systems is also to be ensured within the outsourcing chain.	See row 32, above.
36.	The supervised company must have the possibility of quickly accessing at all times its data stored with the cloud service provider and of re-transferring the same if required. In this regard it has to be ensured that the selected form of re-transfer does not restrict or exclude the use of the data. For that reason, platform-independent standard data formats should be agreed. Compatibility of the different system must be taken into account.	See row 29, above.
37.	**6. Termination provisions**	
38.	Termination rights and adequate termination notice periods are to be agreed. In particular, a special termination right, providing for termination for good cause if the supervisory authority calls for the agreement to be ended, should be agreed.	We provide customers with a broad right to terminate for convenience, which would allow them to terminate in any circumstances.

	Consideration	Atlassian Commentary
39.	It has to be ensured that in the event of termination the items outsourced to the cloud service provider continue to be provided until such time that the outsourced item has been completely transferred to another cloud service provider or to the supervised company. In this regard it has to be guaranteed in particular that the cloud service provider will reasonably assist the supervised company in transferring the outsourced items to another cloud service provider or directly to the supervised company.	If required by an institution, it may extend its subscription term for a short period to enable its transition to another service provider.
40.	The type, form and quality of transfer of the outsourced item and the data should be defined. If data formats are adapted to the individual needs of the supervised company, the cloud service provider should deliver a documentation of such adaptations on termination.	This information is accessible in our **Documentation**.
41.	It should be agreed that after re-transfer of the data to the supervised company its data have been completely and irrevocably deleted on the side of the cloud service provider.	This consideration is addressed in our **Data Processing Addendum**.
42.	To ensure that the outsourced areas are maintained in the event of the planned or unplanned termination of the agreement, the supervised company must have an exit strategy and review its feasibility.	This is a customer consideration.
43.	**7. Chain outsourcing**	
44.	Provisions on the possibility and the modalities of chain-outsourcing ensuring that the requirements of supervisory law continue to be met are to be agreed. Restrictions resulting, e.g., in only the most substantially similar obligations being assumed are not permissible. It must be ensured in particular that the information and audit rights as well as controlling possibilities of the supervised outsourcing company as well as of the supervisory authorities also apply to subcontractors in the case of chain-outsourcing.	In order to provide global products with minimal interruptions, we may sub-outsource certain critical functions to high-quality service providers (e.g., data hosting providers). With respect to critical sub-outsourcings, Atlassian commits to ensuring that it has appropriate contracts with such sub-outsourcers, which grant appropriate audit, access and information rights to institutions and their supervisory authorities, and require such sub-outsourcers to comply with all applicable laws. Please also see row 12, above.

	Consideration	Atlassian Commentary
45.	With a view to chain-outsourcing, reservations of consent of the outsourcing company or specific conditions to be met in order for chain-outsourcing to be possible should be provided for in the outsourcing agreement. It should be defined which outsourced items and/or portions thereof may be chain-outsourced and which ones may not.	See row 44, above.
46.	The supervised company should be informed in advance of chain-outsourcing of the outsourced items and/or portions thereof in text form. The subcontractors and the items and/or portions thereof chain-outsourced to them should be known to the supervised company.	Atlassian will provide notice of any changes to, or new, sub-outsourcing of critical or important functions and provide information about such sub-outsourcings. If the institution has concerns about such sub-outsourcings, we will allow the institution to terminate its contract with us.
47.	In the event of a new chain-outsourcing, it has to be kept in mind that this may have impacts on the risk situation of the outsourcing and thus on the outsourcing company. Accordingly, the risk analysis should at least be reviewed or repeated in the event of a new chain outsourcing. This also applies where material defects as well as material changes in the cloud service provided by subcontractors become known.	This is a customer consideration.
48.	The company should review and monitor the performance of the entire service on an ongoing basis, regardless of whether the cloud service is provided by the cloud service provider or its subcontractors.	This is a customer consideration.
49.	**8. Information duties**	
50.	Provisions are to be agreed ensuring that the cloud service provider informs the supervised company about developments that might adversely affect the orderly performance of the outsourced items. That includes things like reporting any disruptions in providing the cloud service. This is to ensure that the company can adequately monitor the outsourced item.	We publish service availability updates at **https://status.atlassian.com/**, and contractually commit to notifying customers of events that have a material impact on the availability of the Covered Cloud Products.

	Consideration	Atlassian Commentary
51.	The cloud provider is to inform the supervised company without delay about any circumstances that might pose a risk to the security of the supervised company's data to be processed by the cloud service provider, e.g. as a result of acts by third parties (e.g. attachment or confiscation), insolvency or composition proceedings, or other events.	In addition to the commitments referenced in row 50, above, we commit to providing customers with notice of security incidents in our **Data Processing Addendum**.
52.	It should be ensured that the supervised company is adequately informed by the cloud service provider in advance in the event of relevant changes in the cloud service to be provided by the cloud service provider. Service descriptions and any changes to them should be provided and/or notified to the supervised company in text form. It should be ensured that the supervised company is adequately informed, to the extent permitted by law, where any requests/demands for surrender of data of the supervised company are made by third parties.	We publish our **Cloud Product Roadmap**, which provides customers with notice of material changes to the Covered Cloud Products In addition, we only provide customer data to third parties in accordance with our Guidelines for **Law Enforcement Requests.**
53.	**9. Notice of applicable law**	
54.	Where a choice of law clause is agreed and German law is not agreed as the governing law, the law of a country from the European Union or the European Economic Area should at any event be agreed as the law governing the agreement.	The default governing law of Atlassian Customer Contract is California law. Please contact our Enterprise Sales Team for more details.

1The term "material outsourcing" as used in the BaFin Guidance is equivalent to the term "critical or significant outsourcing" as used in the EBA Guidelines.

Learn more about Compliance at Atlassian

ATLASSIAN