ATLASSIAN

EBA Guidelines

The European Banking Authority's guidelines on outsourcing arrangements

LAST UPDATED DEC 2021

The chart below sets out each paragraph in Section 13 (Contractual Phase) of the European Banking Authority's Guidelines on Outsourcing Arrangements (the "**EBA Guidelines**"). To aid your internal review, we have described how we address each of the considerations in the EBA Guidelines. Atlassian's financial services offering covers qualifying customers purchasing the Enterprise editions of the Covered Cloud Products.

	EBA Guidelines Reference	Consideration	Atlassian Commentary
1	**13. Contractual Phase**		
2	Para. 74	The rights and obligations of the institution, the payment institution and the service provider should be clearly allocated and set out in a written agreement.	Generally addressed by the Atlassian customer contract.
3	Para. 75	The outsourcing agreement for critical or important functions should set out at least:	
4		**(a)** a clear description of the outsourced function to be provided;	Our **Documentation**, which is incorporated by reference into the Atlassian customer contract for qualifying customers, contains clear descriptions of the Covered Cloud Products.

	EBA Guidelines Reference	Consideration	Atlassian Commentary
5		**(b)** the start date and end date, where applicable, of the agreement and the notice periods for the service provider and the institution or payment institution;	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.
6		**(c)** the governing law of the agreement;	The default governing law of Atlassian Customer Contract is California law. Please **contact our Enterprise Sales Team** for more details.
7		**(d)** the parties' financial obligations;	The pricing for each of the Covered Cloud Products is published on **atlassian.com**
8		**(e)** whether the sub-outsourcing of a critical or important function, or material parts thereof, is permitted and, if so, the conditions specified in Section 13.1 (Sub-outsourcing of critical and important functions) that the sub-outsourcing is subject to;	Refer to the comments on Section 13.1 in rows 21 through 36.
9		**(f)** the location(s) (i.e. regions or countries) where the critical or important function will be provided and/or where relevant data will be kept and processed, including the possible storage location, and the conditions to be met, including a requirement to notify the institution or payment institution if the service provider proposes to change the location(s);	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.

	EBA Guidelines Reference	Consideration	Atlassian Commentary
10		**(g)** where relevant, provisions regarding the accessibility, availability, integrity, privacy and safety of relevant data, as specified in Section 13.2 (Security of data and systems);	Refer to the comments on Section 13.2 in rows 36 through 39.
11		**(h)** the right of the institution or payment institution to monitor the service provider's performance on an ongoing basis;	We publish service availability updates at **status.atlassian.com**, and contractually commit to notifying customers of events that have a material impact on the availability of the Covered Cloud Products.
12		**(i)** the agreed service levels, which should include precise quantitative and qualitative performance targets for the outsourced function to allow for timely monitoring so that appropriate corrective action can be taken without undue delay if the agreed service levels are not met;	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**.
13		**(j)** the reporting obligations of the service provider to the institution or payment institution, including the communication by the service provider of any development that may have a material impact on the service provider's ability to effectively carry out the critical or important function in line with the agreed service levels and in compliance with applicable laws and regulatory requirements and, as appropriate, the obligations to submit reports of the internal audit function of the service provider;	We publish service availability updates at **status.atlassian.com**, and contractually commit to notifying customers of events that have a material impact on the availability of the Covered Cloud Products.
14		**(k)** whether the service provider should take mandatory insurance against certain risks and, if applicable, the level of insurance cover requested;	Atlassian maintains insurance coverages against a number of identified risks and as required by Laws that are applicable to our business.

	EBA Guidelines Reference	Consideration	Atlassian Commentary
15		**(l)** the requirements to implement and test business contingency plans;	We maintain business continuity plans and disaster recovery plans, as **described on our Trust Center.** These plans are reviewed and tested at least annually.
16		**(m)** provisions that ensure that the data that are owned by the institution or payment institution can be accessed in the case of the insolvency, resolution or discontinuation of business operations of the service provider;	We allow the customer to access and export its data throughout the duration of our contract. Neither of these commitments are disapplied on Atlassian's insolvency. Nor does Atlassian have the right to terminate for Atlassian's own insolvency - although the customer can elect to terminate for convenience in this scenario. In the unlikely event of Atlassian's insolvency, the customer can refer to these commitments when dealing with the appointed insolvency practitioner.
17		**(n)** the obligation of the service provider to cooperate with the competent authorities and resolution authorities of the institution or payment institution, including other persons appointed by them;	Atlassian will cooperate with the institution's competent authorities and resolution authorities in their exercise of their audit, information and access rights.
18		**(o)** for institutions, a clear reference to the national resolution authority's powers, especially to Articles 68 and 71 of Directive 2014/59/EU (BRRD), and in particular a description of the 'substantive obligations' of the contract in the sense of Article 68 of that Directive;	Atlassian understands that institutions and any resolution entity must be able to carry on business during resolution. To provide support through resolution, we commit to continue providing the Covered Cloud Products during resolution as required by the BRRD.
19		**(p)** the unrestricted right of institutions, payment institutions and competent authorities to inspect and audit the service provider with regard to, in particular, the critical or important outsourced function, as specified in Section 13.3 (Access, information and audit rights); and	Refer to the comments on Section 13.3 in rows 40 through 53.

	EBA Guidelines Reference	Consideration	Atlassian Commentary
20		**(q)** termination rights, as specified in Section 13.4 (Termination rights).	Refer to the comments on Section 13.4 in row 56.
21	**13.1 Sub-outsourcing of critical or important functions**		
22	Para. 76	The outsourcing agreement should specify whether or not sub-outsourcing of critical or important functions, or material parts thereof, is permitted	In order to provide global products with minimal interruptions, we may sub-outsource certain critical or important functions to high-quality service providers (e.g., data hosting providers).
23	Para. 77	If sub-outsourcing of critical or important functions is permitted, institutions and payment institutions should determine whether the part of the function to be sub-outsourced is, as such, critical or important (i.e. a material part of the critical or important function) and, if so, record it in the register	This is a customer consideration.
24	Para. 78	If sub-outsourcing of critical or important functions is permitted, the written agreement should:	
25		**(a)** specify any types of activities that are excluded from sub-outsourcing;	See row 22, above.
26		**(b)** specify the conditions to be complied with in the case of sub-outsourcing;	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.

	EBA Guidelines Reference	Consideration	Atlassian Commentary
27		**(c)** specify that the service provider is obliged to oversee those services that it has sub-contracted to ensure that all contractual obligations between the service provider and the institution or payment institution are continuously met;	Atlassian remains responsible for its overall performance under the Atlassian customer contract, including for any functions that are sub-outsourced. In addition, with respect to critical or important 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 competent authorities and resolution authorities, and require such sub-outsourcers to comply with all applicable laws.
28		**(d)** require the service provider to obtain prior specific or general written authorisation from the institution or payment institution before sub-outsourcing data;	As part of our compliance with the **GDPR**, in our **DPA**, we commit to not engaging any subprocessors to process Customer Personal Data without a customer's prior written consent.
29		**(e)** include an obligation of the service provider to inform the institution or payment institution of any planned sub-outsourcing, or material changes thereof, in particular where that might affect the ability of the service provider to meet its responsibilities under the outsourcing agreement. This includes planned significant changes of sub-contractors and to the notification period; in particular, the notification period to be set should allow the outsourcing institution or payment institution at least to carry out a risk assessment of the proposed changes and to object to changes before the planned sub-outsourcing, or material changes thereof, come into effect;	See row 26, above.
30		**(f)** ensure, where appropriate, that the institution or payment institution has the right to object to intended sub-outsourcing, or material changes thereof, or that explicit approval is required;	See row 26, above.

	EBA Guidelines Reference	Consideration	Atlassian Commentary
31		**(g)** ensure that the institution or payment institution has the contractual right to terminate the agreement in the case of undue sub-outsourcing, e.g. where the sub-outsourcing materially increases the risks for the institution or payment institution or where the service provider sub-outsources without notifying the institution or payment institution.	See row 26, above.
32	Para. 79	Institutions and payment institutions should agree to sub-outsourcing only if the subcontractor undertakes to:	
33		**(a)** comply with all applicable laws, regulatory requirements and contractual obligations; and	See row 27, above.
34		**(b)** grant the institution, payment institution and competent authority the same contractual rights of access and audit as those granted by the service provider.	See row 27, above.
35	Para. 80	Institutions and payment institutions should ensure that the service provider appropriately oversees the sub-service providers, in line with the policy defined by the institution or payment institution. If the sub-outsourcing proposed could have material adverse effects on the outsourcing arrangement of a critical or important function or would lead to a material increase of risk, including where the conditions in paragraph 79 would not be met, the institution or payment institution should exercise its right to object to the sub-outsourcing, if such a right was agreed, and/or terminate the contract.	See rows 26 and 27, above.

	EBA Guidelines Reference	Consideration	Atlassian Commentary
36	**13.2 Security of data and systems**		
37	Para. 81	Institutions and payment institutions should ensure that service providers, where relevant, comply with appropriate IT security standards	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: **atlassian.com/trust/compliance**
38	Para. 82	Where relevant (e.g. in the context of cloud or other ICT outsourcing), institutions and payment institutions should define data and system security requirements within the outsourcing agreement and monitor compliance with these requirements on an ongoing basis.	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: **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.
39	Para. 83	In the case of outsourcing to cloud service providers and other outsourcing arrangements that involve the handling or transfer of personal or confidential data, institutions and payment institutions should adopt a risk-based approach to data storage and data processing location(s) (i.e. country or region) and information security considerations.	This is a customer consideration.

	EBA Guidelines Reference	Consideration	Atlassian Commentary
40	Para. 84	Without prejudice to the requirements under the Regulation (EU) 2016/679, institutions and payment institutions, when outsourcing (in particular to third countries), should take into account differences in national provisions regarding the protection of data. Institutions and payment institutions should ensure that the outsourcing agreement includes the obligation that the service provider protects confidential, personal or otherwise sensitive information and complies with all legal requirements regarding the protection of data that apply to the institution or payment institution (e.g. the protection of personal data and that banking secrecy or similar legal confidentiality duties with respect to clients' information, where applicable, are observed).	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: **atlassian.com/trust/compliance/resources/gdpr**
41	**13.3 Access, information and audit rights**		
42	Para. 85	Institutions and payment institutions should ensure within the written outsourcing arrangement that the internal audit function is able to review the outsourced function using a risk-based approach.	Atlassian provides institutions with contractual mechanisms to review the Covered Cloud Products on an on-going basis.
43	Para. 86	Regardless of the criticality or importance of the outsourced function, the written outsourcing arrangements between institutions and service providers should refer to the information gathering and investigatory powers of competent authorities and resolution authorities under Article 63(1)(a) of Directive 2014/59/EU and Article 65(3) of Directive 2013/36/EU with regard to service providers located in a Member State and should also ensure those rights with regard to service providers located in third countries.	Atlassian acknowledges the information gathering and investigatory powers of competent authorities and resolution authorities under the relevant and applicable EU legislation.

	EBA Guidelines Reference	Consideration	Atlassian Commentary
44	Para. 87	With regard to the outsourcing of critical or important functions, institutions and payment institutions should ensure within the written outsourcing agreement that the service provider grants them and their competent authorities, including resolution authorities, and any other person appointed by them or the competent authorities, the following: **(a)** full access to all relevant business premises (e.g. head offices and operation centres), including the full range of relevant devices, systems, networks, information and data used for providing the outsourced function, including related financial information, personnel and the service provider's external auditors ('access and information rights'); and **(b)** unrestricted rights of inspection and auditing related to the outsourcing arrangement ('audit rights'), to enable them to monitor the outsourcing arrangement and to ensure compliance with all applicable regulatory and contractual requirements.	For all institutions that use the Covered Cloud Products, Atlassian provides the required audit, information and access rights to institutions, their competent authorities and their designees.
45	Para. 88	For the outsourcing of functions that are not critical or important, institutions and payment institutions should ensure the access and audit rights as set out in paragraph 87(a) and (b) and Section 13.3, on a risk-based approach, considering the nature of the outsourced function and the related operational and reputational risks, its scalability, the potential impact on the continuous performance of its activities and the contractual period. Institutions and payment institutions should take into account that functions may become critical or important over time.	See row 44, above.

	EBA Guidelines Reference	Consideration	Atlassian Commentary
46	Para. 89	Institutions and payment institutions should ensure that the outsourcing agreement or any other contractual arrangement does not impede or limit the effective exercise of the access and audit rights by them, competent authorities or third parties appointed by them to exercise these rights.	Our audit program is designed to allow qualifying customers and their competent authorities to audit the Covered Cloud Products effectively.
47	Para. 90	Institutions and payment institutions should exercise their access and audit rights, determine the audit frequency and areas to be audited on a risk-based approach and adhere to relevant, commonly accepted, national and international audit standards.	We have developed an audit program that is consistent with this consideration.
48	Para. 91	Without prejudice to their final responsibility regarding outsourcing arrangements, institutions and payment institutions may use: **(a)** pooled audits organised jointly with other clients of the same service provider, and performed by them and these clients or by a third party appointed by them, to use audit resources more efficiently and to decrease the organisational burden on both the clients and the service provider; **(b)** third-party certifications and third-party or internal audit reports, made available by the service provider.	Our audit program permits institutions to review the Covered Cloud Products using pooled audits and/or third party certifications.
49	Para. 92	For the outsourcing of critical or important functions, institutions and payment institutions should assess whether third-party certifications and reports as referred to in paragraph 91(b) are adequate and sufficient to comply with their regulatory obligations and should not rely solely on these reports over time.	This is a customer consideration.

	EBA Guidelines Reference	Consideration	Atlassian Commentary
50	Para. 93	Institutions and payment institutions should make use of the method referred to in paragraph 91(b) only if they: **(a)** are satisfied with the audit plan for the outsourced function; **(b)** ensure that the scope of the certification or audit report covers the systems (i.e. processes, applications, infrastructure, data centres, etc.) and key controls identified by the institution or payment institution and the compliance with relevant regulatory requirements; **(c)** thoroughly assess the content of the certifications or audit reports on an ongoing basis and verify that the reports or certifications are not obsolete; **(d)** ensure that key systems and controls are covered in future versions of the certification or audit report; **(e)** are satisfied with the aptitude of the certifying or auditing party (e.g. with regard to rotation of the certifying or auditing company, qualifications, expertise, reperformance/verification of the evidence in the underlying audit file); **(f)** are satisfied that the certifications are issued and the audits are performed against widely recognised relevant professional standards and include a test of the operational effectiveness of the key controls in place;	Sub-paragraphs (a) through (f) are customer considerations.
		(g) have the contractual right to request the expansion of the scope of the certifications or audit reports to other relevant systems and controls; the number and frequency of such requests for scope modification should be reasonable and legitimate from a risk management perspective; and	With respect to sub-paragraph (g), we provide institutions with a contractual mechanism to request modifications to our audit controls and processes.

	EBA Guidelines Reference	Consideration	Atlassian Commentary
		(h) retain the contractual right to perform individual audits at their discretion with regard to the outsourcing of critical or important functions.	Sub-paragraph (h) is addressed in row 44, above.
51	Para. 94	In line with the EBA Guidelines on ICT risk assessment under the SREP, institutions should, where relevant, ensure that they are able to carry out security penetration testing to assess the effectiveness of implemented cyber and internal ICT security measures and processes. Taking into account Title I, payment institutions should also have internal ICT control mechanisms, including ICT security control and mitigation measures.	Atlassian offers customers the right to carry out penetration testing at any time without Atlassian's prior approval: **atlassian.com/trust/security/security-testing**
52	Para. 95	Before a planned on-site visit, institutions, payment institutions, competent authorities and auditors or third parties acting on behalf of the institution, payment institution or competent authorities should provide reasonable notice to the service provider, unless this is not possible due to an emergency or crisis situation or would lead to a situation where the audit would no longer be effective.	Our audit program is tailored for this consideration.
53	Para. 96	When performing audits in multi-client environments, care should be taken to ensure that risks to another client's environment (e.g. impact on service levels, availability of data, confidentiality aspects) are avoided or mitigated.	It is extremely important to Atlassian and our customers that what we do with one customer should not put any other customers at risk. This applies when you perform an audit. It also applies when any other customer performs an audit. When an institution performs an audit we will work with them to minimize the disruption to our other customers. Just as we will work with another auditing customer to minimize the disruption to the institution. In particular, we will be careful to comply with our security commitments at all times.

	EBA Guidelines Reference	Consideration	Atlassian Commentary
54	Para. 97	Where the outsourcing arrangement carries a high level of technical complexity, for instance in the case of cloud outsourcing, the institution or payment institution should verify that whoever is performing the audit – whether it is its internal auditors, the pool of auditors or external auditors acting on its behalf – has appropriate and relevant skills and knowledge to perform relevant audits and/or assessments effectively. The same applies to any staff of the institution or payment institution reviewing third-party certifications or audits carried out by service providers.	This is a customer responsibility.
55	**13.4 Termination Rights**		
56	Para. 98	The outsourcing arrangement should expressly allow the possibility for the institution or payment institution to terminate the arrangement, in accordance with applicable law, including in the following situations: **(a)** where the provider of the outsourced functions is in breach of applicable law, regulations or contractual provisions; **(b)** where impediments capable of altering the performance of the outsourced function are identified; **(c)** where there are material changes affecting the outsourcing arrangement or the service provider (e.g. sub-outsourcing or changes of sub-contractors); **(d)** here there are weaknesses regarding the management and security of confidential, personal or otherwise sensitive data or information; and	We provide customers with a broad right to terminate for convenience, which would allow them to terminate in any of the instances listed in Section 13.4 of the EBA Guidelines.

	EBA Guidelines Reference	Consideration	Atlassian Commentary
		(e) where instructions are given by the institution's or payment institution's competent authority, e.g. in the case that the competent authority is, caused by the outsourcing arrangement, no longer in a position to effectively supervise the institution or payment institution.	We provide customers with a broad right to terminate for convenience, which would allow them to terminate in any of the instances listed in Section 13.4 of the EBA Guidelines.
57	Para. 99	The written outsourcing arrangement should:	
58		**(a)** clearly set out the obligations of the existing service provider, in the case of a transfer of the outsourced function to another service provider or back to the institution or payment institution, including the treatment of data;	We provide all customers with in-product functionality to export their data at any time during the term of their contract without our assistance.
59		**(b)** set an appropriate transition period, during which the service provider, after the termination of the outsourcing arrangement, would continue to provide the outsourced function to reduce the risk of disruptions; and	If required by an institution, it may extend its subscription term for a short period to enable its transition to another service provider.
60		**(c)** include an obligation of the service provider to support the institution or payment institution in the orderly transfer of the function in the event of the termination of the outsourcing agreement.	See rows 58 and 59, above.

ATLASSIAN