Product Specific Terms

Product	Ibexa Cloud
Product description	Ibexa Cloud is a cloud hosting platform that enables Customer to host their Cohesivo installation in the cloud by using the Platform as a Service. The Customer acknowledges and agrees that this Product cannot be used independently and requires an active subscription to a Cohesivo software license.
Services provision	PaaS license
Deployment model	**Authorized PaaS third-party** Upsun- 22 rue de Palestro, 75002 Paris – France Upsun is responsible for provisioning the technical platform required to install the Product, including the database, web server, and supporting infrastructure. The Customer is responsible for installing the Product on the platform instance provisioned by Upsun and for operating the Product within that environment. The Provider does not operate the infrastructure layer of the platform, which is provisioned and managed by Upsun.
Version	2026 Sep

ARTICLE 1. SERVICES TERMS 3
1.1 HOSTING INFRASTRUCTURE SERVICES TERMS 3
1.2 ACCEPTABLE USE 4
1.3 CUSTOMER CONTENT 6
1.4 OPEN-SOURCE SOFTWARE 7
1.5 OBSERVABILITY SUITE SERVICES 7
1.6 CUSTOMER DATA UPON CONTRACT TERMINATION 9
ARTICLE 2. FEES AND PAYMENT 9
2.1 PRICE CHANGES AND OVERAGE 9
ARTICLE 3. LIABILITY 9
ARTICLE 4. EXPORT CONTROL AND ANTI-BRIBERY 10
ARTICLE 5. SERVICE LEVEL AGREEMENT 10
5.1 SCOPE AND COVERAGE 10
5.2 INCLUDED AND EXCLUDED SERVICES 11
5.3 SUPPORT PROCESS 11
5.4 PRIORITY LEVELS 12
5.5 BLACKFIRE SUPPORT 13
5.6 CHANNELS 13
5.7 HOURS 13
5.8 SERVICE LEVELS 13
5.9 PENALTIES 14
ARTICLE 6. DATA PROCESSING AGREEMENT 16
6.1 DATA PROCESSING ACTIVITIES 16
6.2 LIST OF SUB-PROCESSORS 16
6.3 SECURITY MEASURES 18

ARTICLE 1. SERVICES TERMS

1.1 HOSTING INFRASTRUCTURE SERVICES TERMS

1.1.1 Service commitments

The Provider shall host and maintain, through its PaaS sub-contractor, the Customer's production environment for the Service Term and in accordance with the Service Level Agreement set out in these Product Specific Terms.

The Provider may, in its sole discretion, retain third parties to provide the infrastructure services which serve as a component of the Services, including the PaaS sub-contractor identified above.

1.1.2 Additional server resource and storage capacity

On the enterprise dedicated plans, and grid bundles (G-XL and G-2XL plans), the Customer agrees that should the Provider, or its PaaS sub-contractor becomes aware that Customer's servers have or will become overloaded due to greater than normal usage, the Provider, or its sub-contractor will then take reasonable actions to increase the server resource capacity in an effort to maintain project performance. On the grid, upsizes of capacity require a deployment.

The Customer agrees to keep the master branch of their project in a deployable state and acknowledges that a deployment will cause downtime equal to the length of the deploy hook. The Customer agrees that the Provider can unilaterally elect to add capacity for additional storage and computing power up to four times the contracted (as long as a plan four times the capacity of the original exists as a generally available product offer) and that the excess capacity will remain provisioned for a minimum of seven (7) days. Such additional capacity will be billed at then-current rates in weekly increments.

The Provider or its PaaS sub-contractor will also make reasonable efforts to contact the Customer and create a support ticket when it is determined that a server upgrade is needed. For server upgrade needs longer than one month, the required increase will result in a permanent upgrade fee and additional Order Forms or amendments to this Contract may be implemented.

The Provider reserves the right to not provision additional server capacity, if it determines that additional capacity is unlikely to significantly improve performance, including, without limitation, when the overload is caused by an error in the Customer Developments (e.g., PHP code), or during a denial-of-service attack. Required storage increase will result in a permanent upgrade fee.

1.1.3 Reversibility

The Customer has license and/or ownership of, and direct ability to access, at all times to the following (including without limitation):

- Application code (excluding Cohesivo)
- Database
- Uploaded files
- Project configuration files (*.yaml)

1.1.4 Downgrades

The Customer may not downgrade their plan, server resource and storage capacity during the Service Term. Downgrade requests are excluded for dedicated projects and shall only be possible for grid projects at the end of the Service Term, provided the Customer provides the Provider with minimum seventy (70) days written notice prior to the end of the Service Term. Downgrading the plan, server resource and storage capacity may cause loss of the Customer Data, features, or capacity of the Services and the Provider's liability for such loss is excluded. Downgrades are excluded at all times for dedicated projects.

1.2 ACCEPTABLE USE

Customer may not, nor permit the Customer's Users or others within the Customer's control to: copy, republish, reverse engineer, decompile, disassemble or otherwise attempt to discover the source code or underlying ideas or algorithms of the Services; modify, translate, or create derivative works based on the Services; rent, lease, distribute, sell, resell, assign, or otherwise transfer intellectual property rights of the Services; use the Services for time sharing or service bureau purposes or otherwise for the benefit of a third party; remove any trademark or proprietary notices from the Services; or publish or disclose to third parties any evaluation of the Services without

the Provider's prior written consent and only to the extent of such authorized disclosure. The Customer may not interfere with, modify, disrupt or disable features or functionality of Ibexa Cloud, including without limitation any mechanism used to restrict or control the functionality, or defeat, avoid, bypass, remove, deactivate or otherwise circumvent any software protection or monitoring mechanisms of the Services.

The Customer may not use the Services: a) in any way that knowingly violates any applicable law or regulation (including, without limitation, the GDPR and any laws regarding the export of data or software); b) for the purpose of exploiting, harming or attempting to exploit or harm minors in any way by exposing them to inappropriate content, asking for personally identifiable information or otherwise; c) to transmit, or procure the sending of, any advertising or promotional material that may be considered "junk mail", "chain letter" or "spam" or any other similar solicitation; d) to knowingly infringe or violate the intellectual property rights or proprietary rights, rights of publicity or privacy, or other rights of any third party; e) in any way that is harmful, fraudulent, deceptive, threatening, abusive, harassing, tortious, defamatory, vulgar, obscene, libellous or unlawful; f) to impersonate or attempt to impersonate the Provider, an employee of the Provider, another user or any other person or entity (including, without limitation, by using e-mail addresses or screen names associated with any of the foregoing); or g) to knowingly engage in any other conduct that restricts or inhibits anyone's use of the Services, or which, as determined by the Provider, may harm the Provider or users of the Services or expose them to liability.

Additionally, the Customer agrees not to: a) use any robot, spider or other automatic device, process or means to access the Services or any of their content for any purpose, including monitoring or copying any of the material or providing any competing services; b) use any manual process to monitor or copy any of the material made available through the Services, or for any other unauthorized purpose, without the Provider's prior written consent; c) use any device, software or routine that knowingly interferes with the proper working of the Services; d) introduce any viruses, trojan horses, worms, logic bombs or other material which is malicious or technologically harmful; e) attempt to gain unauthorized access to, or knowingly interfere with, damage or disrupt any part of the Services, the infrastructure on which they are hosted, or any server, computer or database connected to the Services; or f) attack the Services via a denial-of-service attack or a distributed denial-of-service attack.

1.3 CUSTOMER CONTENT

Customer represents and warrants that the Customer Data shall not include anything that the Provider may determine in its sole discretion to be or constitute: a) unlawful, offensive, threatening, harmful, libellous, malicious, defamatory, pornographic, obscene, racist, infringing or otherwise objectionable; b) not wholly owned by or validly licensed to the Customer; c) fraud or a violation of a third party's privacy or intellectual property rights; d) a breach of the Contract; e) interference or attempted interference with the proper working of the Services or the Provider's infrastructure; f) promotion or facilitation of gambling, illegal export, or discrimination based on race, sex, religion, nationality, disability, sexual orientation, age or otherwise; g) transmission of viruses, unauthorized data, malware, trojan horses, spyware, worms or other harmful or corrupted components; or h) impersonation, or collection of personally identifying or other information about other customers of the Provider or their users, or use of information obtained from or through the Services, for the purpose of direct marketing, spamming, unsolicited contacting, phishing or pharming. The Provider reserves the right, but shall be under no obligation, to refuse, modify or remove such Customer Data.

Content published through the Services must be published together with the Customer's name, address, telephone number and email address to which questions, complaints or claims from users, customers or others should be directed.

The Customer shall defend, indemnify and hold the Provider and its officers, directors, employees, vendors, agents and Affiliates harmless against claims or suits (including attorneys' fees and expenses) arising out of or resulting from the Customer Data or a breach of the Contract (including, but not limited to, any unauthorized or illegal use or distribution of the Services).

Customer grants to the Provider and its relevant sub-suppliers a non-exclusive, non-transferable, royalty-free, worldwide licence to reproduce, distribute, publicly perform, publicly display and digitally perform the Customer Data only on or in conjunction with a site hosted on Ibexa Cloud. Subject to the foregoing licence, as between the Provider and the Customer, the Customer is and will remain the sole and exclusive owner of all right, title and interest in and to the Customer Data.

1.4 OPEN-SOURCE SOFTWARE

Certain items of software made available through the Services may be open-source software. Such open-source software is not subject to the terms and conditions of this Contract. Each item of open-source software is licensed under such terms of the end-user license that accompanies such open-source software.

1.5 OBSERVABILITY SUITE SERVICES

Blackfire Content: data collected and aggregated from Customer's servers or local machines by the Blackfire Service to the Blackfire website (www.blackfire.io), or directly uploaded by the Customer or Blackfire User, excluding personal data.

Blackfire Service: the performance management solution allowing Customer's Users to test, set and reach performance expectations for their web applications.

Blackfire User: any Customer's User designated by the Customer as beneficiary of a user account ("User Account") and allowed to access and use the Blackfire Service.

1.5.1 Use of the Blackfire Service

The Customer and their Blackfire User agree to comply at all times with the technical requirement or configuration recommendations as shared by the Provider in the documentation or otherwise made available to the Customer and Blackfire User.

A User Account must be created with the Ibexa Cloud Customer account and is mandatory to use the Blackfire Service. User Accounts are personal and shall not be shared between several persons.

The Customer guarantees that the Blackfire Content does not include personal data or personally identifiable information and that the Customer's User has been granted all rights and licenses required for using the data collected by or uploaded to the Blackfire Service.

The Blackfire Service is granted for use on projects hosted on Ibexa Cloud only. Any use on sites or applications not hosted on Ibexa Cloud is excluded.

The Blackfire Service and support provide ways to share the Customer's Users feedback and ideas. The Customer's Users represent and guarantee that they have, or have been granted, any rights and licenses required to submit the feedback and hereby

transfer such rights and licenses to UPSUN who may commercially or non-commercially exploit in any manner, any and all feedback, without any further claim from the Customer.

1.5.2 Customer Data and Blackfire Content

The Blackfire Service is hosted by Amazon SAS in the European Union. The Provider may, at its sole discretion, decide to change from Platform-as-a-Service provider and may consequently have to relocate and process Customer Data and Blackfire Content in another country. In such an event the Customer will be notified thirty (30) days in advance. It is important to note that by default the Blackfire Service does not send any of the Customer project's private data to the Blackfire Service servers (e.g. database content and query parameters). Only the profiling information is sent to the Blackfire Service servers.

The Blackfire Service offers ways to share the Blackfire Content from the Blackfire website. By setting the Blackfire Content to be viewed publicly, the Customer understands and agrees that this Blackfire Content may be viewed by any visitor of the Blackfire website, may they have an account or not, and indexed by search engines. It is the Customer's sole responsibility to share the Blackfire Content publicly, publish the related unique URL giving read access to the Blackfire Content and cease sharing the Blackfire Content to disable anybody to access to it.

The Customer and/or Blackfire Users are solely responsible for the use and implementation of means to ensure the security, protection and backup of their equipment, their Blackfire Content and software. As such, the Customer and/or Blackfire Users undertake to take all appropriate measures to protect their Blackfire Content.

The Provider may anonymize the Blackfire Content and process it for statistical and research purposes.

Expiry or termination of the Contract results in the immediate deletion of the User Account along with all Customer Data and Blackfire Content.

1.5.3 Beta feature

The Provider may occasionally offer to Blackfire Users to experiment beta features. Beta features may be modified, removed or discontinued at the Provider's sole discretion.

1.5.4 No reversibility

Expiry or termination of the Contract results in the immediate deletion of the Blackfire User Account along with all Customer Data and Blackfire Content.

1.6 CUSTOMER DATA UPON CONTRACT TERMINATION

It is Customer's sole responsibility to carry out any reversibility operation (such as deletion, backup, transfer to another hosting provider, etc.) necessary for the conservation or deletion of the Customer Data.

ARTICLE 2. FEES AND PAYMENT

2.1 PRICE CHANGES AND OVERAGE

Provider will be entitled to pass through to the Customer any increase in fees imposed by its Platform-as-a-Service provider, at the then-current fees, for the Renewal Service Term.

ARTICLE 3. LIABILITY

In addition to the Liability clause of the GTC, in no event shall the Provider or its subcontractors, licensors, Affiliates or subsidiaries, and their respective officers, directors, employees and agents, be liable to the Customer or to any third party, including any End User, for any special, punitive or exemplary damages, or for any loss of savings, data files or programs, arising out of the use of or inability to use the Services or in connection with the Contract, even if the Customer or the Provider has been advised of the possibility of such damages. The exclusions and limitations of liability set out in the Contract apply to the fullest extent permitted by law, in all actions of any kind, whether based on contract, tort or any other legal or equitable theory. Each such exclusion and limitation is intended to be separately enforceable, without regard to the other exclusions and limitations, and without regard to whether any other remedy under the Contract fails of its essential purpose.

ARTICLE 4. EXPORT CONTROL AND ANTI-BRIBERY

The Customer represents and warrants that it is not a restricted party (e.g. an individual or entity that has been denied import or export privileges) and will comply with all applicable export control laws, regulations and trade sanctions, including those issued by the United Nations Security Council, the US Government, the European Union or its Member States, the UK Government, the Government of Canada and the Government of Australia. The Customer further represents and warrants that: (i) it will not directly or indirectly use, or allow the Customer's Users to use, the Services in a prohibited country (e.g. Cuba, Iran, North Korea, South Sudan and Syria) or engage in any export or re-export activity with any entity or individual who the Customer knows or has reason to know is engaging in the design, development or production of nuclear, chemical or biological weapons, or missile technology; and (ii) none of the Customer, its Affiliates, or any of its directors, officers or employees, and none of the Customer's Users, is a sanctioned person.

Each Party shall comply with applicable laws concerning anti-bribery and anti-corruption, which may include the US Foreign Corrupt Practices Act of 1977 and the UK Bribery Act 2010.

ARTICLE 5. SERVICE LEVEL AGREEMENT

5.1 SCOPE AND COVERAGE

By way of derogation from Article 1 of the Service Level Agreement, Support is available for all Customer environments hosted on Ibexa Cloud (production, staging and development environments). The service levels and Service Credits only apply to production environments, once the production go-live has been notified by the Customer. Priority 1 (P1) tickets are only applicable to live production environments.

Only Support Contacts will be authorized to submit tickets and exercise the rights for Support granted by the Contract. Project administrators can grant and remove access in the Ibexa Cloud portal and are responsible for managing and maintaining access on

the Customer account. The Provider takes no responsibility for undesired access caused by the Customer's assignment of user access.

5.2 INCLUDED AND EXCLUDED SERVICES

Support includes: a) Response: the Provider will respond to, and make commercially reasonable efforts towards resolving, submitted support tickets relating to consistently reproducible issues, within the time frames corresponding to the Customer's subscribed plan; and b) Post-issue analysis: for Enterprise plans, the Provider will use commercially reasonable efforts to provide, upon request made via an update to the original ticket within fourteen (14) calendar days of the closure of a P1 ticket, a written summary of no more than 500 words (code samples excluded) explaining, as applicable, the circumstances, change or context that caused the issue, or business practices that resolved it, and recommendations for the prevention of future instances. The depth of analysis is at the Provider's discretion and no additional efforts on the issue will be undertaken.

Except as expressly agreed in writing by the Provider, the following are excluded from Support: a) P1 support for non-production, staging, sandbox or other environments related to the development of a production site; b) support for the Customer's End Users, which will be provided exclusively by the Customer; c) support related to application implementation, standard usage and project consulting, unless specifically identified and itemized in the Order Form or a statement of work; and d) installation, configuration, use, maintenance or functionality of non-Service hardware, operating systems, third-party software, databases, networks or other enabling technologies.

5.3 SUPPORT PROCESS

Customers subscribing to Ibexa Cloud benefit from a central point of contact for all Support requests, whether they relate to Cohesivo or to Ibexa Cloud, through the Ibexa Cloud Support Portal. The front desk will verify that the request comes from a Customer eligible for Support, verify and update the Customer's contact data, and qualify whether the request relates to Cohesivo, to Ibexa Cloud and its underlying infrastructure, or both. Requests relating to Cohesivo will be handled by the Cohesivo product support team in accordance with the Cohesivo Product Specific Terms, with the same service

level. Requests relating to Ibexa Cloud and its underlying infrastructure will be handled by the Ibexa Cloud support team in accordance with this Service Level Agreement.

Tickets must be submitted separately for each project and issue and should include a description of the issue or request, a description of the desired state or outcome, the steps necessary to demonstrate or reproduce the issue, and an initial indication of the priority level. The initial response will include a confirmation of receipt, the validation or modification of the priority level indicated by the Customer (with an explanation, if applicable) and, where necessary, a request for additional information. Ticket statuses are: New (not yet reviewed), Open (analysis in process), Pending (awaiting feedback or other progress from the Customer) and Solved (concluded either through resolution of the issue or a determination that no further work is warranted).

Information provided by the Customer in the Ibexa Cloud Support Portal must be accurate, complete and up to date. The Customer is responsible for maintaining the confidentiality of its passwords, shall notify the Provider if their security has been compromised, and accepts full responsibility for activity conducted through the Support Portal in breach of this confidentiality obligation.

5.4 PRIORITY LEVELS

Priority levels for Ibexa Cloud are defined as follows. Response targets do not necessarily include the initiation of resolution or ultimate resolution targets.

Priority 1 Urgent (P1): a catastrophic production problem that severely impacts the Customer's production systems, or because of which the Customer's production systems are down or not functioning, or that results in a loss of production data, and for which no workaround exists. The Provider will make continuous efforts, with appropriate escalation to senior management, to provide a resolution.

Priority 2 High (P2): a problem in which the Customer's system is functioning but in a reduced capacity, or the problem is causing significant impact to portions of business operations and productivity, or the software is exposed to potential loss or interruption of service. The Provider will make continuous efforts to provide a resolution.

Priority 3 Normal (P3): a medium- to low-impact problem that involves partial and/or non-critical loss of functionality, or that impairs some operations but allows the Customer's operations to continue to function, including problems with limited or no

loss of functionality or impact for which there is an easy workaround. The Provider will use reasonable efforts to provide a resolution in time for the next minor release of the software.

Priority 4 Low (P4): a low- to very-low-impact problem, or a general question, that does not impair the Customer's operations.

5.5 BLACKFIRE SUPPORT

Blackfire support begins on the Effective Date as stated in the Order Form, or another date as mutually agreed to by both Parties and will expire on the last day of the then current Service Term. Blackfire support tickets will be addressed 24/7/365 as per the procedure set forth in this Service Level Agreement. All Blackfire support tickets will be treated as Priority 3 Normal (P3) tickets.

5.6 CHANNELS

Support requests shall be submitted through the Ibexa Cloud Support Portal available on the Ibexa Cloud online interface.

5.7 HOURS

Support begins on the Effective Date as stated in the Order Form, or another date as mutually agreed by the Parties, and expires on the last day of the then current Service Term. Support tickets are addressed 24/7/365, in order of priority, within the response times set out below.

5.8 SERVICE LEVELS

5.8.1 Service uptime

Component	Enterprise Grid	Enterprise Dedicated
Platform-as-a-Service (production)	99.9%	99.99%

The Provider will use commercially reasonable efforts to make Ibexa Cloud available at the agreed uptime, as measured over each calendar month, taking into account only

interruptions labelled as Priority 1 (P1) incidents and excluding incidents labelled as P2, P3 or P4 and Scheduled Maintenance. Downtime means the inability of the Provider's PaaS sub-contractor to run projects due either to errors or failures in the hosting stack or to a lack of network connectivity to the Internet. The PaaS sub-contractor shall not be considered a third-party provider for the purposes of the exclusions in Article 4.1 of the Service Level Agreement.

Uptime is measured against the incident reports generated by the PaaS sub-contractor after each interruption of service, a copy of which the Provider shall provide to the Customer upon request. The Customer may monitor the availability of the Platform-as-a-Service by subscribing to the PaaS sub-contractor's status page, where Scheduled Maintenance may also be announced in advance when possible.

5.8.2 First Response Time

First Response Time is measured 24x7x365.

Priority	Estimated Response Time
P1	< 1 h
P2	8 h
P3	24 h
P4	48 h

5.9 PENALTIES

Service Credits are calculated as a percentage of the total charges paid for Ibexa Cloud for the affected production project for the month in which the unavailability occurred, as follows:

Monthly Uptime Percentage	Enterprise Grid (99.9% SLA)	Enterprise Dedicated (99.99% SLA)
Greater than or equal to 99.99%	0%	0%

Below 99.99% to 99.90%	0%	3%
Below 99.90% to 99.80%	5%	5%
Below 99.80% to 99.70%	5%	10%
Below 99.70% to 99.50%	10%	20%
Below 99.50% to 99.00%	20%	33%
Below 99.00% to 97.00%	30%	33%
Below 97.00%	50%	50%

To receive a Service Credit the Customer must submit a claim by notifying the Provider's Support in writing within sixty (60) days after the incident occurred, including: the words "SLA Credit Request" in the subject line; the dates and times of each incident when the Service was not available and for which credit is claimed; all necessary system identification information (such as the project ID); and request logs that document the errors and corroborate the claimed outage (with any confidential or sensitive information removed or replaced with asterisks). If the Monthly Uptime Percentage is confirmed by the Provider and is less than the agreed uptime, the Provider will issue the Service Credit. Failure to provide the credit request and other information as required above will disqualify Service Credit eligibility.

Service Credits will only be applied against future payments otherwise due; the Provider may, at its discretion, apply them to the Customer's open balance. Service Credits do not entitle the Customer to any refund or other payment, will only be issued if the credit amount for the applicable month is greater than €10, $10 or £10 (depending on the contract currency), are forfeited twelve (12) months after issuance and may not be transferred or applied to any other account. Unless otherwise specified in writing or required by law, Service Credits are the Customer's sole and exclusive remedy for any unavailability, non-performance or other failure by the Provider to provide hosting-related services.

ARTICLE 6. DATA PROCESSING AGREEMENT

6.1 DATA PROCESSING ACTIVITIES

Item	Description
Purpose and nature of processing	Provision, operation, security, maintenance and support of the Services, including hosting, storage, transmission, backup, deletion of personal data, or other processing activities depending on the Customer's use of the Services..
Categories of personal data	The categories of personal data are determined by the Customer and may vary depending on the Customer's use of the Services.
Categories of data subjects	The categories of data subjects are determined by the Customer and may vary depending on the Customer's use of the Services.
Duration of processing	Personal data shall be processed for the duration of the Contract and for as long as determined by the Customer through its use of the Services, including until the Customer deletes the personal data or instructs the Processor to do so.

6.2 LIST OF SUB-PROCESSORS

UPSUN

Item	Description

About	A Platform-as-a-Service (PaaS)
Registered offices	22 rue de Palestro, 75002 Paris – France
Contact	sayhello@upsun.com
Processing purpose	Processing of customer data is carried out to provide the Upsun Services, including hosting, deploying, operating and maintaining customer applications and environments, providing support, ensuring service availability and security, and fulfilling contractual and legal obligations
Processing location	Customer project data is stored in the region selected by the customer and, according to Upsun, project data does not leave that region unless the customer requests an additional dedicated cluster in another location. Backups remain in the same region. Access logs may be transferred to a collection point within the EU for security and availability purposes. Upsun also uses subprocessors located both inside and outside the EU, with appropriate contractual safeguards such as SCCs where required
Security measures	Upsun implements technical and organizational security measures including encryption of data in transit and at rest, TLS/SSH, access controls, 2FA support, security monitoring, vulnerability scanning and penetration testing, backups, firewall protection and restricted internal access to customer data. Upsun states that its security controls are independently assessed and that it maintains ISO/IEC 27001, SOC 2 Type 2 and PCI DSS Level 1 compliance

JIRA

Item	Description
About	https://www.atlassian.com/software/jira
Registered offices	Atlassian Pty Ltd, Level 6, 341 George St, Sydney NSW 2000, Australia
Contact	privacy@atlassian.com
Processing purpose	Issue escalation to level 2 support and to development teams
Processing location	Data residency configured in Europe (Frankfurt, Germany)
Security measures	• https://www.atlassian.com/trust/security/security-practices • https://www.atlassian.com/trust/data-protection • Atlassian maintains ISO/IEC 27001 certification and SOC 2 compliance reports. • Encryption in transit and at rest.

6.3 SECURITY MEASURES

Platform as a Service is provided by our technology partner Upsun. Ibexa will ensure that Upsun implements appropriate technical and organizational measures within the scope of its scope of services in addition to the measures taken by Ibexa itself.

Details of Upsun's technical and organizational measures can be found in the section "Technical and organizational measures in Annex III" of the online document: https://upsun.com/trust-center/privacy/dpa/

Upsun is dedicated to an annual SOC 2 Type II audit. An abridged version of the audit report is available upon request. Upsun is ISO 27001 certified.