Data Processing Agreement

Version: 2026 Oct

Ibexa AS, Askekroken 11, 0277 Oslo, Norway

ARTICLE 1. PURPOSE AND SCOPE 3
ARTICLE 2. ROLES OF THE PARTIES 3
ARTICLE 3. DEFINITIONS AND INTERPRETATION 4
ARTICLE 4. PROCESSING INSTRUCTIONS 4
ARTICLE 5. COMPLIANCE WITH DATA PROTECTION LAWS 5
ARTICLE 6. SPECIAL CATEGORIES OF PERSONAL DATA 5
ARTICLE 7. CONFIDENTIALITY 5
ARTICLE 8. SECURITY MEASURES 5
ARTICLE 9. USE OF SUB-PROCESSORS 5
ARTICLE 10. USE OF THIRD-PARTY BY THE CONTROLLER 6
ARTICLE 11. INTERNATIONAL DATA TRANSFERS 6
ARTICLE 12. ASSISTANCE TO THE CONTROLLER 7
ARTICLE 13. REGULATORY DISCLOSURE 7
ARTICLE 14. DATA SUBJECT RIGHTS 7
ARTICLE 15. PERSONAL DATA BREACH 7
ARTICLE 16. AUDIT AND COMPLIANCE VERIFICATION 8
16.1 AUDIT 8
16.2 PENETRATION TEST 9
ARTICLE 17. DATA RETENTION 9
ARTICLE 18. DATA PROTECTION OFFICER 10

ARTICLE 1. PURPOSE AND SCOPE

This Data Processing Agreement ("DPA") is entered between the Customer ("Controller") and the Provider ("Processor"). This DPA forms part of and is incorporated by reference into the Contract between the Parties.

This DPA governs the processing of Customer personal data by the Processor on behalf of the Controller in connection with the provision of the Services.

The Processor shall not act as a Controller or joint controller for the processing covered by this DPA.

ARTICLE 2. ROLES OF THE PARTIES

The Customer acknowledges and agrees that it is solely responsible for determining the legal basis for the processing of Customer personal data, including personal data relating to its employees, personnel, agents and for providing all required notices and obtaining any necessary consents as required by applicable data protection laws.

The Provider may provide Support directly to the Customer's Users solely for the purpose of delivering the Services. In this context, the Provider shall process any personal data exchanged strictly as a Processor acting on behalf of the Customer and shall not use such personal data for its own purposes, except where such data is aggregated and anonymized or otherwise processed in accordance with applicable law.

The Provider may provide authentication services across multiple Products subscribed to by the Customer, including through Single Sign-On (SSO) functionality. For this purpose, the Provider may process the Customer's Users' identifiers and related account information solely to authenticate users, recognize linked accounts, and facilitate access across such Products.

Notwithstanding the foregoing, the Provider shall act as an independent Controller with respect to personal data processed for its own legitimate business purposes, including but not limited to:

- account management and administration of the Customer relationship;
- billing, invoicing and payment processing;
- financial accounting, tax compliance and record-keeping obligations;

- maintaining the security, integrity and operation of the Provider's underlying infrastructure;
- fraud prevention, abuse detection and enforcement of the Contract; and
- compliance with applicable legal and regulatory obligations.

For the avoidance of doubt, personal data processed by the Provider in its capacity as independent Controller, is processed for the Provider's own purposes and is not subject to the terms of this DPA, except where applicable law requires otherwise.

ARTICLE 3. DEFINITIONS AND INTERPRETATION

All terms defined in the General Data Protection Regulation (GDPR - Regulation (EU) 2016/679 of 27 April 2016) have the meaning given to them in the GDPR, unless otherwise defined in this DPA. In case of conflict, data protection laws prevail over contractual provisions.

ARTICLE 4. PROCESSING INSTRUCTIONS

The Processor shall process personal data only on documented instructions from the Controller. Instructions are deemed documented through this DPA, the Product Specific data processing activities and legitimate use of the Services. The Processor shall inform the Controller if an instruction infringes applicable data protection laws.

In accordance with the regulations, the Processor undertakes to process the personal data only to the extent necessary for the purposes of performing the Services. Except with the express, prior and written agreement of the Controller, the Processor refrains from processing the personal data for other purposes not provided for in the Contract.

ARTICLE 5. COMPLIANCE WITH DATA PROTECTION LAWS

Each party shall comply with its respective obligations under applicable data protection laws. The Processor shall implement appropriate internal policies and measures to ensure compliance with this DPA and the GDPR.

ARTICLE 6. SPECIAL CATEGORIES OF PERSONAL DATA

The Controller shall refrain from processing special categories of personal data as defined in Article 9 of the GDPR. Should the Controller choose to process such data, it shall do so at its sole responsibility, ensuring compliance with all applicable requirements, including obtaining the data subject's explicit consent, conducting Data Protection Impact Assessments (DPIA) and implementing appropriate technical and organizational security measures.

ARTICLE 7. CONFIDENTIALITY

The Processor shall ensure that all personnel with access to personal data are subject to a duty of confidentiality and receive appropriate data protection training.

ARTICLE 8. SECURITY MEASURES

The Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including measures addressing confidentiality, integrity, availability, and resilience. Details are described in each Product Specific Terms.

ARTICLE 9. USE OF SUB-PROCESSORS

The Controller authorizes the Processor to engage sub-processors listed in the applicable Product Specific Terms.

The Processor may appoint additional sub-processors for specific processing activities and shall notify the Controller of any intended additions or replacements. Such notice shall include the relevant processing activities and the identity and contact details of the sub-processor. The Controller may object within thirty (30) days of receiving the notice, being understood that these objections must be of a reasonable nature.

If the Controller does expressly object to the change of sub-processor within the aforementioned conditions and deadline and if no solution could be found, the

Controller may decide to terminate the agreement with the Processor by giving thirty (30) business days written notice. In this case, the Controller shall pay the Processor for all services already performed on its behalf until the effective date of termination.

ARTICLE 10. USE OF THIRD-PARTY BY THE CONTROLLER

The Processor may recommend certain third-parties to the Controller, particularly to allow for the transfer of personal data between the Processor and the third-party. The Controller remains solely responsible for any third-party it configures or activates and shall ensure that it enters appropriate data processing agreement with such third-parties.

ARTICLE 11. INTERNATIONAL DATA TRANSFERS

Transfers of personal data outside the EEA shall occur only where lawful transfer mechanisms are in place, such as adequacy decisions or standard contractual clauses.

ARTICLE 12. ASSISTANCE TO THE CONTROLLER

The Processor shall assist the Controller, considering the nature of the processing, with:

- responding to data subject requests;
- conducting data protection impact assessments;
- consultations with supervisory authorities;
- demonstrating compliance under Articles 28 and 32–36 GDPR.

Such assistance shall be limited to what is reasonable and proportionate and shall not require the Processor to incur disproportionate effort.

ARTICLE 13. REGULATORY DISCLOSURE

Any disclosure of personal data by the Processor to a supervisory authority shall be strictly limited to cases where such disclosure is mandated under union or member state law. The Processor shall notify the Controller without undue delay, unless prohibited by law, and shall ensure that any disclosure is proportionate, documented, and legally justified.

ARTICLE 14. DATA SUBJECT RIGHTS

The Processor shall promptly notify the Controller of any data subject request received directly and shall not respond unless authorized. The Processor shall provide reasonable assistance to enable the Controller to fulfil its obligations.

ARTICLE 15. PERSONAL DATA BREACH

The Processor will notify the Controller of any personal data breach affecting the Controller, without undue delay. This information will be as complete as possible to allow the Controller to meet his own notification obligations within seventy-two (72) hours. In that event, the Processor must notably describe the nature of the data breach, the approximate number of data subjects concerned, the likely consequences, as well as the measures taken to remedy the breach.

ARTICLE 16. AUDIT AND COMPLIANCE VERIFICATION

16.1 AUDIT

Scope and frequency of audits

The Data Controller (including all its affiliated companies and entities within the same group) may carry out only one (1) audit per period of twelve (12) consecutive months.

Conditions

If the Controller requests an audit related to personal data protection and/or security, the Controller shall (i) notify the Processor at least five (5) business days prior to such audit by email to security@ibexa.co (ii) ensure that such procedure does not unreasonably interfere with the Processor business and operations.

The notification will be accompanied by a document mentioning the rules of engagement which will precisely include the following points: (i) the scope of the audit; (ii) the objective of the audit; (iii) the areas of the audit (as defined by ISO 27001, ISO 27701, ISAE 3000 or any equivalent auditing methodology); (iv) the name and contact details of the appointed auditors and (v) the audit schedule.

The Processor will have the right to request a review of the rules of engagement on (i) the competence and/or independence/impartiality of the auditors, (ii) the timing of the audit, (iii) the scope of the audit if the Processor is concerned that the audit may affect the service provided to its customers.

Security and risk assessment questionnaires

In order to avoid a large number of informal requests, all requests for assessments, compliance checks or security questionnaires issued by the Data Controller or any of its entities/affiliates must be centralised and sent exclusively to security@ibexa.co. The Data Processor undertakes to complete one (1) standard annual questionnaire on the security and protection of personal data per twelve (12)-month period, provided that the information requested is not already covered by certifications, third-party audit reports (e.g. ISO 27001, ISAE 3000) or documentation made available by the Data Processor.

Expenses and cost allocation

The costs of any audit or additional questionnaire shall be borne by the Data Controller. Any on-site audit, additional audit or response to security questionnaires exceeding the annual limit (or requiring bespoke responses not covered by the Processor's standard documentation) will be invoiced to the Data Controller.

The Controller shall provide the Processor with a copy of the audit report and allow the Processor to respond to it. The audit and its results shall not be construed as an

acknowledgement of liability, of any security or confidentiality breach, or as a commitment by the Processor to remedy any issue identified in the audit.

16.2 PENETRATION TEST

Upon written request, the Processor shall provide the Controller with the executive summary of the last penetration test report where applicable.

To protect the integrity, availability and security of the Product, the Controller shall not, and shall not allow any third party to, conduct any penetration test without the Processor's prior written consent.

ARTICLE 17. DATA RETENTION

The Processor shall retain Personal Data only for the duration necessary to provide the Services and as instructed by the Controller, unless retention is required by law.

Upon termination of the Contract, the Processor shall, at the Controller's choice, return or securely delete all personal data, unless legally required to retain it. Certification of deletion shall be provided upon request.

ARTICLE 18. DATA PROTECTION OFFICER

In accordance with article 37 of the GDPR, the Processor has appointed a data protection officer, who can be contacted at the following email address: privacy@ibexa.co.

The Controller shall, if applicable, appoint a data protection officer and share this information with the Processor by any means possible. Failing this, the Controller's contact person will be also registered as the contact person for all matters relating to personal data protection.