

BIG Data Processing Agreement

Oct 9, 2026

This Data Processing Agreement ("DPA") governs the processing of personal data that Dataminds A/S carries out on behalf of its customers as data processor in connection with the BIG platform. The DPA applies when the customer accepts it or starts using BIG, unless a separately signed data processing agreement between the parties replaces it.

The DPA is entered into pursuant to Article 28(3) of Regulation (EU) 2016/679 of the European Parliament and of the Council ("GDPR").

Parties

The data controller:

The customer that has entered into a cooperation agreement or another agreement with Dataminds A/S on the use of BIG (the "Main Agreement"), as identified by name, address and company registration number in the Main Agreement.

The controller's contact person for data protection matters is the person designated in the Main Agreement. If no such person is designated, the person who signed the Main Agreement on behalf of the controller is the contact person. The controller shall keep the contact details up to date by notifying the processor at mail@dataminds.com.

The data processor:

Dataminds A/S

Ankersgade 12C, 1, 8000 Aarhus C, Denmark

CVR: 31186935

Contact: mail@dataminds.com

The parties are hereinafter referred to individually as "the controller" and "the processor" and jointly as "the parties".

1. Preamble

1.1 The terms "personal data", "special categories of personal data", "processing", "data subject", "controller" and "processor" have the meanings given in the GDPR.

1.2 The purpose of this DPA is to ensure the parties' compliance with applicable data protection legislation and to document the controller's instructions to the processor. The processor processes personal data on behalf of the controller solely to provide, operate, secure and support the controller's use of the BIG platform.

1.3 This DPA sets out the rights and obligations of the parties when the processor processes personal data on behalf of the controller.

1.4 This DPA takes precedence over any conflicting provisions on the processing of personal data in other agreements between the parties. Where the parties have signed a separate data processing agreement covering BIG, that agreement supersedes this DPA.

1.5 This DPA does not relieve the processor of obligations imposed on it directly by applicable data protection legislation.

2. Rights and obligations of the controller

2.1 The controller is responsible for ensuring that the processing of personal data in connection with its use of BIG complies with Article 24 GDPR, other applicable EU or national law, and this DPA.

2.2 The controller has the right and obligation to decide the purposes and means of the processing, including which users are given access to BIG.

2.3 The controller is responsible for ensuring a lawful basis for the processing and for any disclosure of personal data that the processor is instructed to carry out, including disclosure to the sub-processors listed in Annex B.

2.4 BIG is designed so that report and analytics data do not contain personal data. The controller shall ensure that data delivered to BIG for reporting purposes does not contain personal data, unless otherwise agreed in writing with the processor. If personal data is nevertheless delivered to BIG, the processor processes it as processor on the controller's instructions and subject to this DPA, and the controller remains responsible for the lawfulness of that processing.

2.5 The controller is responsible for the accuracy, integrity, content and lawfulness of the personal data processed by the processor, and for fulfilling its duty to inform data subjects.

2.6 By entering into this DPA, the controller confirms that the processor has provided sufficient guarantees regarding the technical and organisational measures described in this DPA.

3. The processor acts on instructions

3.1 The processor shall process personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by EU or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. By entering into this DPA, the controller instructs the processor to process personal data:

1. in accordance with applicable law;
2. to provide, operate, secure and support BIG, including user authentication, access management and logging;
3. as further specified through the controller's normal use of BIG;
4. as described in this DPA.

3.2 The processor shall immediately inform the controller if, in its opinion, an instruction infringes the GDPR or other EU or Member State data protection provisions.

4. Security of processing

4.1 The processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, in accordance with Article 32 GDPR.

4.2 The processor shall only grant access to personal data processed on behalf of the controller to persons who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, and only to the extent necessary. The obligation of confidentiality continues after termination of this DPA.

4.3 The processor is certified according to ISO/IEC 27001 (information security) and ISO/IEC 27701 (privacy information management) by Bureau Veritas. In addition, the following measures are of particular importance:

1. Encryption of personal data in transit and at rest.
2. Multi-factor authentication and single sign-on for access to BIG, managed through a central identity provider.
3. Segregation of customer data, so that one customer's data cannot be accessed by another customer.
4. Access to personal data restricted to employees who need it to fulfil the processor's obligations under this DPA.
5. Regular vulnerability scanning and penetration testing.
6. Regular backups and an annual disaster recovery test.
7. Ongoing security and data protection awareness training for all employees.
8. Established controls to detect, handle and report personal data breaches.

9. Change management procedures ensuring that changes to systems, databases and networks are made in a controlled and consistent manner.

5. Use of sub-processors

5.1 The processor uses sub-processors to operate BIG. This DPA constitutes the controller's prior general written authorisation of the processor's use of sub-processors. The sub-processors in use are listed in Annex B.

5.2 The processor shall impose on each sub-processor, by way of a contract or other legal act, data protection obligations equivalent to those set out in this DPA. The processor remains fully liable to the controller for the performance of the sub-processor's obligations.

5.3 The processor shall notify the controller at least 30 days before engaging a new sub-processor or replacing an existing one. The controller may object to the change on reasonable data protection grounds within that period. The processor shall then demonstrate compliance by giving the controller access to its assessment and documentation regarding the sub-processor. If the parties still cannot agree, the controller may terminate its use of BIG with effect from the date the new sub-processor is engaged.

6. Transfers to third countries or international organisations

6.1 BIG is hosted in the EU, and personal data is not transferred to countries outside the EU/EEA as part of the processor's normal operation of BIG. The processor uses Microsoft Azure in accordance with Microsoft's EU Data Boundary commitments.

6.2 Any transfer of personal data to a third country or an international organisation, including support access by a sub-processor from outside the EU/EEA, requires a valid transfer basis under Chapter V GDPR, such as an adequacy decision or the European Commission's Standard Contractual Clauses. The controller authorises the processor to establish such a basis on the controller's behalf.

7. Assistance to the controller

7.1 Taking into account the nature of the processing, the processor shall assist the controller by appropriate technical and organisational measures, insofar as possible, in fulfilling the controller's obligation to respond to requests from data subjects exercising their rights under Chapter III GDPR.

7.2 The processor shall assist the controller in ensuring compliance with Articles 32 to 36 GDPR, including security of processing, notification of personal data breaches to the supervisory authority and to data subjects, data protection impact assessments and prior consultation, taking into account the nature of the processing and the information available to the processor.

7.3 The processor shall not respond to requests from data subjects unless authorised by the controller. The processor shall not disclose personal data to public authorities, including the police, unless required to do so by law, such as by a court order.

7.4 To the extent possible and lawful, the processor shall notify the controller without undue delay if it receives a request from a data subject or from a public authority concerning personal data processed on behalf of the controller.

7.5 The processor may charge the controller for assistance that goes beyond what the processor is required to provide under applicable data protection legislation.

8. Notification of personal data breach

8.1 The processor shall notify the controller without undue delay, and in any event no later than 48 hours, after becoming aware of a personal data breach affecting personal data processed on behalf of the controller.

8.2 The notification shall be sent to the controller's contact person as determined under the section Parties of this DPA. To the extent available, it shall describe the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences, and the measures taken or proposed to address the breach. Information that is not available at the time of notification may be provided in phases.

9. Return and deletion of data

9.1 Before the termination of the controller's use of BIG, and no later than 30 days after termination, the controller may request that the processor return the personal data processed on its behalf in a commonly used electronic format. The processor shall not delete the data before this period has expired, unless the controller requests earlier deletion.

9.2 No later than 90 days after termination, the processor shall delete all personal data processed on behalf of the controller, including copies in backups, unless EU or Member State law requires the processor to retain the data. On request, the processor shall confirm the deletion in writing.

10. Audit and inspection

10.1 The processor shall make available to the controller all information necessary to demonstrate compliance with Article 28 GDPR and this DPA, and shall allow for and contribute to audits, including inspections, conducted by the controller or an auditor mandated by the controller.

10.2 The processor's valid ISO/IEC 27001 and ISO/IEC 27701 certificates, together with related documentation, constitute the primary documentation of the processor's

compliance. The controller shall rely on these before requesting a separate audit of measures already covered by the certifications.

10.3 Any audit or inspection beyond the documentation in clause 10.2 shall be agreed in advance as to scope, timing and duration, shall be carried out during normal business hours with reasonable notice, and is at the controller's expense, including the processor's time spent assisting.

11. Commencement and termination

11.1 This DPA applies for as long as the processor processes personal data on behalf of the controller in connection with the controller's use of BIG.

11.2 After termination of this DPA, the processor may retain personal data only to the extent required by applicable law. Such data shall remain protected by the technical and organisational measures described in this DPA.

12. Changes to this DPA

12.1 The current version of this DPA is available at all times on the processor's website. Material changes shall be notified to the controller by email at least 30 days before they take effect. If the controller does not accept a material change, it may terminate its use of BIG with effect from the date the change takes effect. Continued use of BIG after the changes take effect constitutes acceptance of the updated DPA.

13. Liability

13.1 Each party's liability for breach of this DPA is governed by the general rules of Danish law, subject to the limitations and exclusions of liability in the Main Agreement, which apply to this DPA as if set out in it. This does not limit either party's liability towards data subjects under Article 82 GDPR. The processor is liable for the acts and omissions of its sub-processors as for its own.

14. Governing law and venue

14.1 This DPA is governed by Danish law. Any dispute arising out of or in connection with this DPA shall be brought before the Court of Aarhus (Retten i Aarhus) as the court of first instance.

This DPA was last updated on 9 October 2026, except Annex B, which is updated on an ongoing basis with notice in accordance with clause 5.3.

Annex A – Processing, categories of personal data and data subjects

A. Nature and purpose of the processing

The processor stores and processes user account and log data to authenticate users, manage access, operate and secure BIG, and provide support. Report and analytics data in BIG do not contain personal data (see clause 2.4). Personal data delivered to BIG contrary to clause 2.4 is processed only to store and present it in BIG on the controller's instructions.

B. Categories of personal data

- User account data: name, email address, username, user ID, organisation, and assigned roles and access rights.
- Authentication data: credentials and multi-factor authentication data, stored in protected form.
- Log data: IP address, timestamps, browser and device information, and records of user activity in BIG.

The processor does not process special categories of personal data (sensitive data) as part of BIG.

C. Categories of data subjects

- The controller's employees who are users of BIG.
- Other persons the controller grants access to BIG, such as consultants, partners or the controller's own customers.

D. Duration of the processing

The processing lasts for as long as the controller uses BIG, followed by deletion in accordance with clause 9.

Annex B – List of sub-processors

Name	Company reg. no.	Description of processing	Hosting location
Microsoft Ireland Operations Limited	IE 256796	Microsoft Azure: hosting and infrastructure for BIG.	Ireland (Azure North Europe)