Data Processing Agreement

Last update: June 11th, 2025

Effective date: June 11th, 2025

This Data Processing Agreement ("DPA") forms an integral part of the End User License Agreement ("EULA") between BeZoned and the Licensee for the licensing and purchase of services from BeZoned. By executing the DPA, the Licensee enters into this DPA on behalf of itself and, to the extent required under Applicable Data Protection Laws and Regulations, in the name and on behalf of its Affiliates. This DPA shall be effective when the Licensee accepts the EULA.

This Data Processing Agreement ("DPA") forms the basis for the processing of Personal Data carried out by BeZoned ("Data Processor") on behalf of the Licensee ("Data Controller"). Jointly, the Data Processor and the Data Controller shall be referred to as the Parties.

This DPA is entered into pursuant to Article 28(3) of the General Data Protection Regulation (GDPR) (EU 2016/679) of the European Parliament and Council to regulate BeZoned's processing of Personal Data on behalf of the Licensee.

1. Preamble

1.1 The definitions of "Personal Data," "Special Categories of Personal Data" (sensitive data), "Data Processing," "the Data Subject," "Data Controller," and "Data Processor" are the same as stated in the General Data Protection Regulation (GDPR).

1.2 The purpose of this DPA is to ensure the Parties' compliance with applicable data protection laws and to document the Data Controller's instructions to the Data Processor. The purpose of the Data Processor's processing of Personal Data on behalf of the Data Controller is to facilitate the Data Controller's use of the BeZoned virtual office application as further described in BeZoned's EULA.

1.3 This DPA establishes the Parties' rights and obligations when the Data Processor processes Personal Data on behalf of the Data Controller.

1.4 This DPA takes precedence over other conflicting terms regarding the processing of Personal Data, as outlined in BeZoned's EULA or other agreements between the Parties. The DPA is valid between the Parties as long as the Data Controller subscribes to BeZoned.

1.5 This DPA does not exempt the Data Processor from obligations additionally imposed by applicable data protection laws.

2. The Data Controller's Rights and Obligations

2.1 The Data Controller is responsible for ensuring that the processing of Personal Data in connection with the use of the BeZoned application complies with GDPR Article 24, other EU laws, national laws, and this DPA.

2.2 The Data Controller has the right and the obligation to make decisions about the purposes and means of processing Personal Data. It is solely under the Data Controller's control which Personal Data are processed, including data entered and generated in the BeZoned application.

2.3 The Data Controller is responsible for ensuring that there exists a lawful basis for the processing and sharing of Personal Data that the Data Processor is instructed to carry out, including the sharing of data with sub-processors listed at any given time.

2.4 The Data Controller is responsible for ensuring the accuracy, integrity, reliability, and legality of the Personal Data processed by the Data Processor.

2.5 The Data Controller has fulfilled all mandatory requirements and obligations regarding notifications to or obtaining permission from relevant public authorities concerning the processing of Personal Data.

2.6 The Data Controller has fulfilled its obligation to inform Data Subjects about the processing of their Personal Data in accordance with applicable data protection legislation.

2.7 The Data Controller confirms that the Data Processor has provided the necessary guarantees regarding the implementation of technical and organizational security measures to protect the rights and Personal Data of Data Subjects, as specified in this DPA.

3. The Data Processor Acts on Instructions

3.1 The Data Processor may only process Personal Data according to documented instructions from the Data Controller, unless required by EU or national law to which the Data Processor is subject. By entering into this DPA, the Data Controller instructs the Data Processor to process Personal Data in the following ways:

3.1.1 In compliance with applicable law;

3.1.2 To fulfill its obligations under BeZoned's EULA;

3.1.3 As further detailed by the Data Controller's normal use of the BeZoned application;

3.1.4 As described in this DPA.

3.2 The Data Processor shall immediately notify the Data Controller if an instruction is deemed to be contrary to applicable data protection legislation or other EU or national law.

4. Data Processing Security

4.1 The Data Processor is obligated to maintain a high level of security through the implementation of relevant organizational, technical, and physical security measures. These measures are carried out considering available technology, implementation costs as well as the scope, context, and purpose of processing to ensure an adequate security level that addresses risks and the category of the Personal Data requiring protection.

4.2 The Data Processor may only grant access to Personal Data processed on behalf of the Data Controller to individuals who are bound by confidentiality or appropriate statutory obligations—and only as necessary. This confidentiality obligation shall persist beyond the termination of the DPA.

4.3 BeZoned has implemented numerous security measures and internal data protection policies to ensure the confidentiality, integrity, resilience, and accessibility of Personal Data. These include but are not limited to:

4.3.1 Risk assessments of internal security standards to ensure current technical and organizational measures are sufficient to protect Personal Data, including compliance with GDPR Article 32 on processing security and Article 25 on privacy by design and default.

4.3.2 Effective encryption during the transfer of Personal Data over the internet.

4.3.3 Ongoing awareness training for all employees focused on IT security and Personal Data handling.

4.3.4 External access to systems and databases used for processing Personal Data is strictly regulated via built-in firewalls.

4.3.5 Limiting access to Personal Data to individuals required to comply with the requirements and obligations of the DPA.

4.3.6 Established controls to identify and report potential breaches of Personal Data security.

4.3.7 Regular vulnerability scans and penetration tests to ensure technical measures are implemented and verified effectively.

4.3.8 Procedures ensuring consistent system, database, and network changes to maintain security standards.

5. Use of Sub-processors

5.1 As part of its operations, the Data Processor utilizes sub-processors. This DPA constitutes the Data Controller's prior general written approval for the Data Processor's use of sub-processors. Such sub-processors may include third-party providers both within and outside the EU/EEA. The Data Processor's sub-processors are listed in Annex B.

5.2 The Data Processor ensures that its sub-processors comply with equivalent obligations and requirements as described in this DPA. The Data Controller must be informed at least 30 days before the Data Processor engages a new sub-processor. The Data Controller has the right to object to a new sub-processor processing Personal Data on the Data Controller's behalf if this sub-processor does not handle the data in accordance with applicable data protection legislation. In such a situation, the Data Processor must demonstrate compliance by granting the Data Controller access to the Data Processor's data protection assessment as well as documentation regarding the use of the sub-processor. If disagreement about the use of the sub-processor persists, the Data Controller may terminate their subscription with shorter notice than usual to ensure that the Data Controller's Personal Data is not processed by the sub-processor in question.

6. Transfer Personal Data to Third Countries or International Organizations

6.1 Any transfer of Personal Data to a third country or an international organization requires the conclusion of the EU Commission's Standard Contractual Clauses (EU SCCs) or another valid transfer basis. The Data Controller authorizes the Data Processor to ensure an adequate basis for the transfer of Personal Data to a third country on behalf of the Data Controller.

7. Assistance to the Data Controller

7.1 The Data Processor shall, as far as possible, assist the Data Controller with appropriate technical and organizational measures, taking into account the nature of the processing and the category of data available to the Data Processor, to ensure compliance with the Data Controller's obligations under applicable data protection legislation.

7.2 The Data Processor assists the Data Controller in complying with GDPR Articles 32-36, including, among other things, processing security, reporting breaches of Personal Data security to the supervisory authority, and notifying the Data Subject of such breaches, taking into account the nature of the processing and the information available to the Data Processor.

7.3 The Data Processor must not respond to requests from Data Subjects unless authorized to do so by the Data Controller. The Data Processor will not disclose information about this DPA to government authorities, such as the police, including Personal Data, unless required by law in the form of a court order or similar. In such cases, the Data Processor must inform the Data Controller without undue delay.

7.4 Furthermore, the Data Processor shall, as far as possible and legally permissible, notify the Data Controller if:

7.4.1 A request for access to Personal Data is received directly from the Data Subject;

7.4.2 A request for access to Personal Data is received directly from government authorities, including the police, unless the Data Processor is instructed not to notify the Data Controller.

7.5 If the Data Controller requires information or assistance regarding security measures, documentation, or information about how the Data Processor generally processes Personal Data, and

such request includes information that exceeds what is necessary according to applicable data protection legislation, the Data Processor may charge for such additional services.

8. Notification of Personal Data Security Breaches

8.1 The Data Processor shall notify the Data Controller without undue delay upon becoming aware of a breach of personal data security involving Personal Data processed by the Data Processor on behalf of the Data Controller. This notification is intended to support the Data Controller in meeting their obligations related to such security breaches, including fulfilling the Data Controller's obligation under GDPR Article 33 or other applicable law or regulation to notify the relevant supervisory authority and data subjects about security breaches.

8.2 The Data Processor will deliver notification(s) of Personal Data security breach(es) to the Data Controller by any means the Data Processor selects, including via email. It is the Data Controller's sole responsibility to ensure that Data Controller maintains accurate contact information with the Data Processor. Data Controller is solely responsible for complying with its obligations under incident notification laws applicable to Data Controller and fulfilling any third-party notification obligations related to any security breach or incident.

8.3 The Data Controller must notify the Data Processor without undue delay upon becoming aware of any possible misuse of its accounts or authentication credentials or any security incident related to the Data Processor's products and services.

9. Data Retention and Deletion

9.1 At all times during the term of the Data Controller's subscription, the Data Controller will have the ability to access, extract and delete Customer Data stored in the BeZoned application.

9.2 If the Data Controller terminates the subscription, the Data Controller will have the ability to extract Customer Data before the end of the subscription term. After the end of the subscription term, the Data Processor will delete or anonymize Customer Data and Personal Data.

9.3 Data Processor has no liability for the deletion of Customer Data or Personal Data as described in this section.

10. Audit, including Inspection

10.1 The Data Controller is entitled to initiate an audit of the Data Processor's obligations under the DPA.

10.2 If the Data Processor's assistance with the audit exceeds the standard service that the Data Processor is required to provide under applicable data protection laws, this assistance will be billed separately.

11. Effective Date and Termination

11.1 This DPA remains in effect as long as the Data Processor processes Personal Data on behalf of the Data Controller in connection with the Data Controller's use of the BeZoned application.

11.2 The Data Processor is entitled to retain Personal Data after the termination of the DPA to the extent required by applicable law. In such case, Personal Data will be safeguarded in accordance with the technical and organizational security measures described in this DPA.

12. Changes to the DPA

12.1 The current version of the DPA can always be accessed on BeZoned's website. The Data Controller will be notified about material changes 30 days before such changes take effect. The Data Processor will deliver such notification(s) to the Data Controller by any means the Data Processor selects, including via email. It is the Data Controller's sole responsibility to ensure that Data Controller maintains accurate contact information with the Data Processor. Use of the BeZoned application after the changes have taken effect constitutes acceptance of the changes to the DPA.

13. Liability

13.1 Liability for actions in violation of the provisions of this DPA is governed by the liability provisions of the BeZoned EULA. This also applies to any breach committed by the Data Processor's subcontractors.

14. Governing Law

14.1 This Agreement is governed by the laws of Denmark, without regard to its conflict of law principles. The United Nations Convention on Contracts for the International Sale of Goods (CISG) shall not apply to this Agreement. Disputes may be resolved at the Data Processor's discretion:

- In the courts of the User's jurisdiction; or

- By arbitration administered by The Danish Institute of Arbitration in Copenhagen, Denmark, in English.

Annex A – Categories of Personal Data and Data Subjects

A. Categories of Personal Data

The Data Controller is in control of what categories of Personal Data are processed in the BeZoned application. These categories may include:

- User Identification & Contact Details
  - Full name, display name, user principal name, and unique directory IDs
  - Business e-mail address
  - Organization, department, title and other profile attributes
- Authentication & Access Credentials
  - Sign-in tokens / identifiers used to authenticate the user
- Presence & Availability Data
  - Current presence state, status message, last-seen timestamp
- Group, Team, Channel & Membership Information
  - Team, group and channel names, descriptions, settings
  - Membership lists and role assignments
  - Creation and deletion events for teams, groups and channels
- Communication Content & Metadata
  - 1-to-1 and group chat messages (body, attachments, reactions, timestamps)
  - Channel messages and posts
  - E-mails sent by the service on behalf of users
  - Call set-up data, meeting invitations, join information
- Audio, Video & Real-Time Media
  - Live audio/video streams of calls and meetings
  - Recordings of online meetings
  - AI-generated meeting transcripts
    (These data may include the voices and likenesses of participants.)
- Files & Documents
  - Files stored in SharePoint/OneDrive sites that the user or team can access
  - Tabs content or configuration that embed documents (File contents are only processed as required to provide in-app viewing, search or collaboration features.)
- Application Configuration & Installation Data
  - Installed Teams apps and their settings
  - Custom tabs, bot configurations, channel or team settings
- Directory & Organisation-Wide Reference Data
  - Tenant-level directory schema, domain names, company-wide settings

In addition to the above categories, Special Categories of Personal Data (sensitive Personal Data) may be processed by the Data Processor if the Data Controller allows such information to be used in the BeZoned application. However, this remains beyond the Data Processor's control.

B. Categories of Data Subjects

The Data Controller is in control of what categories of Data Subjects are processed in the BeZoned application. These categories may include:

- The Data Controller's end-users
- The Data Controller's employees
- The Data Controller's contact persons
- The Data Controller's customers and their end-users
- The Data Controller's customers' employees
- The Data Controller's customers' contact persons
- Others

Annex B – Sub-processors

Below is an overview of BeZoned sub data processors.

BeZoned uses sub-processors for processing Personal Data. These sub-processors are typically providers of cloud services or other IT hosting services. DPAs are in place with all of BeZoned's sub-processors to protect the Data Controller's data as best as possible.

If sub-processors are located outside the EU, we make sure to have a valid transfer basis in place, including entering into the EU's Standard Contractual Clauses (SCC).

Sub data processor	Product	Hosting location	Purpose
Microsoft Ireland Operations Limited	Microsoft Azure, Microsoft Teams	Holland, Ireland	Storage of data files, user names, passwords. BeZoned is an add-in to Microsoft Teams. Users will already be working on Microsoft Teams and have accepted Microsoft's terms, DPA, and Privacy Policy. The use of BeZoned will not result in the storage of any data in excess of what the user has already agreed with Microsoft.

Contact us if you have any questions

If you have any questions regarding our use of sub data processors, feel free to reach out to us at privacy@bezoned.com.