Version: 12th November 2024

Data Processing Agreement

1 Processing Operations and Definitions

(1) This Data Processing Agreement ("**DPA**") supplements the Contract identified in **Appendix 1** to this DPA and applies to all Processing operations regarding Personal Data and here whenever the Contractor identified in **Appendix 1** to this DPA ("**Processor**"), its employees or sub-contractors (as applicable) may come into contact with Personal Data Processed by the Processor on behalf of the Customer identified in **Appendix 1** to this DPA ("**Controller**") as part of the provision of Services within the meaning of **Appendix 1** under the Contract identified therein. The subject-matter and duration, the nature and purposes of Processing, the types of Personal Data and the categories of Data Subjects are listed in **Appendix 1** to this DPA, which may differentiate between specific Services provided.

(2) All capitalized terms, and their equivalent (e.g. Personal Data and Personal Information carry the same meaning), used in this DPA, while not defined in this DPA or elsewhere in the Contract, but defined in the General Data Protection Regulation (EU 2016/679 – "**GDPR**") or other laws and regulations for protection of personal data, as applicable (collectively "**Data Protection Laws**"), including US state Personal Data Protection Acts including the CCPA, shall have the meaning as defined in the applicable Data Protection Laws. "**CCPA**" means the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights and Enforcement Act of 2020 and any other applicable amendments (codified at § Cal. Civ. Code 1798.100 et seq.), and includes any and all implementing regulations and any revisions or superseding laws and regulations including the California Privacy Rights Act ("**CPRA**"). This DPA reflects each party's understanding and agreement with regard to the Processing of Personal Data and applies only where required by an applicable Data Protection Laws.

2 Processing on Behalf of the Controller

(1) The Processor shall Process Personal Data on behalf of the Controller only within the scope of the Contract on the Controller's documented instructions, unless statutory obligations require the Processor to Process Personal Data otherwise.

(2) Additional instructions must be issued in writing or in an electronic format (text form). Verbal additional instructions must be confirmed by Controller in writing or in text form immediately.

(3) If the Processor considers an instruction to violate applicable Data Protection Laws, it shall inform the Controller immediately and be entitled to suspend the execution of the relevant instructions until the Controller confirms or changes them.

(4) For purposes of the CCPA, and similar Data Protection Laws as applicable, the Controller shall be considered a "Business" and the Processor shall be considered a "Service Provider". With regard to any Personal Information provided by the Controller to the Processor pursuant to the Contract, the Processor hereby acknowledges and agrees that it shall not (i) "Sell" or "Share" (per CPRA and Data Protection Laws with similar provisions) the Personal Information, (ii) retain, use, or disclose the Personal Information for any purpose other than for the specific purpose of performing the Services pursuant to the documented instructions, or (iii) retain, use, or disclose Personal Information outside of the direct business relationship with the Controller. Without limiting the foregoing, each party acknowledges and agrees that the provision of Personal Information from the Controller to the Processor does not constitute, and is not the intent of either party for such provision of Personal Information to constitute, a "Sale" of Personal Information, and if valuable consideration, monetary or otherwise, is being provided by the Controller pursuant to the Contract, such valuable consideration, monetary or otherwise, is so being provided for the Services being rendered and not for the provision of Personal Information. For purposes of this paragraph 4 only, the terms "Business," "Service Provider," "Personal Information," "Sale," and "Sell" shall have the same meaning as set forth in the CCPA (Cal. Civ. Code § 1798.140). The limitations set forth in this paragraph 4 shall not be interpreted to prevent the Processor from complying with an applicable law, statute, regulation, or a binding order of a governmental or regulatory body.

3 Obligations of the Processor

(1) The Processor shall not use the Controller's Personal Data in the scope of this DPA for any purpose other than described in the Contract and to fulfil its obligations under the Contract.

(2) At any time during the Processing, the Processor shall correct, delete or block Personal Data in the scope of this DPA where the Controller issues such instruction.

(3) The Processor's personnel engaged in performing Processing operations under this DPA shall be bound to confidentiality, unless they are already under an appropriate statutory obligation of confidentiality.

(4) The Processor shall notify to the Controller the point of contact for all issues related to data privacy and protection within the scope of the Contract.

(5) The Processor shall periodically monitor its internal processes and the technical and organizational measures to ensure that Processing within its area of responsibility is in accordance with the applicable Data Protection Laws.

(6) The Processor shall reasonably assist the Controller in complying with its obligations according to Art. 32 to 36 GDPR or the corresponding obligations under other applicable Data Protection Laws.

(7) The Processor may Process Personal Data within or outside a Member State of the European Union ("**EU**") or the European Economic Area ("**EEA**"). Every transfer of Personal Data to a state which is not a Member State of either the EU or the EEA shall only occur if the specific conditions of Art. 44 et seqq. GDPR or the corresponding provisions of other applicable Data Protection Laws have been fulfilled.

(8) Upon Controller's request, and as otherwise required by Data Protection Laws, Processor shall (at Controller's sole cost and expense) provide Controller with commercially reasonable cooperation and assistance (i) needed to fulfil Controller's obligation under applicable Data Protection Laws to undertake a

data protection impact assessment related to Controller's use of the services, to the extent Controller does not otherwise have access to the relevant information, and to the extent such information is available to Processor and (ii) with respect to a consultation with a government or regulatory authority.

4 Obligations of the Controller

(1) The Controller shall ensure compliance with the statutory provisions of the applicable Data Protection Laws, in particular the lawfulness of the Processing of Personal Data by the Processor on behalf of the Controller.

(2) The Controller shall inform the Processor immediately, but no later than within forty-eight (48) hours, in case the Controller detects any errors or irregularities of the Processing operations which affect the compliance with the applicable Data Protection Laws.

5 Data Subject's Rights

(1) The Processor is not obliged to directly respond to any enquiries of Data Subjects and shall refer such Data Subjects to the Controller, if the information provided by the Data Subject suffices to identify the Controller the enquiry relates to. The foregoing applies accordingly, where a Data Subject requests the Processor to correct, delete or block data.

(2) If the Controller is obliged to answer any Data Subjects' enquiry related to the Processing of Personal Data, the Processor shall reasonably support the Controller in providing the required information. The Processor shall only be obliged to provide the information upon the Controller's documented instruction. The Processor shall not be liable if the Controller fails to correctly or timely respond to the request of the concerned Data Subject, or if the Controller does not respond to the Data Subject's enquiries at all.

(3) If claims pursuant to Art. 82 GDPR or the corresponding provisions of other applicable Data Protection Laws are brought by the Data Subject against the Processor, the Controller undertakes to reasonably assist the Processor's defense against such claims.

6 Technical and Organizational Measures

(1) The Processor will implement and maintain the technical and organizational measures set out in **Appendix 2** to this DPA, which may differentiate between specific Services provided.

(2) The technical and organizational measures are subject to technical progress and further development. The Processor may amend the technical and organizational measures, provided that the new measures do not fall short of the level of security provided by the specified measures. Substantial changes must be documented.

7 Communication in the Case of Personal Data Breaches

The Processor shall notify the Controller without undue delay if the Processor becomes aware of any Personal Data breach relating to the Controller's Personal Data and provide reasonably available information needed by the Controller to meet its notification obligations towards the Data Subject and/or reporting obligations towards competent data protection authorities. The Controller instructs the Processor to take all measures the Processor deems necessary or helpful to secure the Personal Data Processed on behalf of the Controller and to minimize any possible adverse consequences to the Data Subject.

8 Sub-contracting

(1) The Processor may not sub-contract any or a portion of the Processing of Personal Data to sub-processors without the Controller's prior specific or general written consent. The Controller hereby specifically consents to the Processor engaging the sub-processors in the Processing of Personal Data on behalf of the Controller as provided in **Appendix 1** to this DPA, which may differentiate between specific Services provided. The Controller hereby generally consents to the Processor engaging further sub-processors who provide sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the Processing of Personal Data will meet the requirements of the GDPR or the corresponding requirements of other applicable Data Protection Laws.

(2) The Processor shall inform the Controller of any intended addition or replacement of sub-processors covered by **Appendix 1** to this DPA, thereby giving the Controller the opportunity to object to the change. The Controller shall promptly notify the Processor in writing within fourteen (14) days as of the receipt of the Processor's notification, if and on which reasonable grounds it objects to the substitute or additional sub-processor.

(3) If the Controller does not timely object, it will be deemed to have consented to the addition or replacement of sub-processors covered by **Appendix 1** to this DPA. If the Controller objects, the Processor is entitled to either terminate this DPA by providing thirty (30) days' prior written notice to the Controller, or to use reasonable efforts to propose to the Controller a change in the Processing operations to avoid Personal Data being Processed by the additional or substitute sub-processor. The suggested change may not unreasonably burden the Controller. If the Processor chooses to suggest a change in the Processing operations and the Processor is then unable to execute the change within a reasonable period of time, or if the Controller does not approve the suggested change, while such approval may not be unreasonably withheld, either party may terminate the DPA by providing thirty (30) days' prior written notice to the other party.

(4) When engaging sub-processors in the Processing of Personal Data on behalf of the Controller, the Processor shall ensure the fulfilment of the following conditions:

- The sub-processing contract must reflect the data protection provisions agreed between the Controller and the Processor in this DPA;
- The Processor is responsible for the conduct and performance of each approved sub-processor, and will be the Controller's sole point of contact regarding the Processing of Personal Data by the sub-processor.

9 Audit Rights

(1) Upon prior written request, the Processor will certify to the Controller that it is in compliance with this DPA by providing adequate evidence in form of the results of a self-audit, internal company rules of conduct including external evidence of compliance, certificates on data protection and/or information security (e. g. ISO 27001), approved codes of conduct, or other appropriate certificates. Evidence of the implementation of measures which are not specific to this DPA may be given in the form of up-to-date attestations, reports or extracts thereof from independent bodies (e.g. external auditors, internal audit, the data protection officer, the IT security department or quality auditors) or suitable certification by way of an IT security or data protection audit.

(2) The Controller has the right to audit the Processor's compliance with this DPA, if the Controller believes, based on reasonable grounds to be notified to the Processor, that the rights under paragraph 1 are not sufficient in an individual case, or a competent data protection authority requests an audit. The audit shall only be carried out during normal business hours without disruption of the Processor's business operations, taking into account a reasonable lead time, which shall in no case be less than thirty (30) days. The Processor may make the audit conditional upon the signing of a confidentiality agreement with regard to the data of other customers and the technical and organizational measures taken.

(3) The Controller may not appoint a third-party auditor that is in a competitive relationship with the Processor or its affiliates or not suitably qualified to conduct the audit. The Controller will not exercise its audit rights more than once in any twelve (12) months period, except (i) if and when required by instruction of a competent data protection authority or other regulator with jurisdiction over the Controller; or (ii) the Controller reasonably believes a further audit is necessary due to a breach or suspected breach of security suffered by the Processor.

(4) The Processor is under no obligation to disclose or provide access to any (i) data related to other customers of (x) the Processor, (y) its affiliates, or (z) any sub-processors; (ii) of the Processor's, its affiliates' or any sub-processors' internal accounting or financial information or trade secrets; or (iii) information that could compromise the security of any systems or business facilities of the Processor's, its affiliates or any sub-processors.

10 Return or Deletion of Personal Data Upon Termination

Upon the termination of this DPA, the Processor will, at the choice of the Controller, delete the Personal Data Processed hereunder or return such data and delete existing copies, unless and for as long as applicable law requires storage of such data.

11 Miscellaneous

In case of a contradiction, the provisions of this DPA shall take precedence over the other provisions of the Contract, insofar as the contradiction concerns the Processing of Personal Data; otherwise, the other provisions of the Contract shall prevail.

Appendix 1 to the DPA

Certain Personal Data- and Processing-Related Information:

Subject-matter of Processing of Personal Data	Provision of Services to the Controller under the Contract (each as defined below). The DPA supplements the contract between the Processor and the Controller on the Processor's services which involves, or may involve, Personal Data Processing by the Processor on behalf of the Controller ("**Contract**") with respect to the operation of the BuildingMinds Platform and the provision of the BuildingMinds Platform Services and/or ancillary products or services such as Professional Services (collectively the "**Services**"). The Contract may constitute, and the Services may be provided under (a) an order issued by Controller and confirmed by Processor (which may or may not incorporate the terms of framework agreements between Processor and Controller or their respective Affiliates), or (b) an individually negotiated contract between Processor and Controller or their respective Affiliates. Terms defined in the Contract but not in this DPA shall have the meaning given to them in the Contract, and the terms "**Contractor**" and "**Customer**" shall refer to the parties to such Contract. The respective roles of Contractor and its Affiliates (jointly "**BM Group**") with respect to the Services are set forth below. All members of the BM Group involved in the Personal Data Processing on behalf of the Controller are subject to intercompany agreements which ensure that all members of the BM Group at all times comply with the terms of this DPA. For the purposes of this DPA, the member of the BM Group which is the Contractor under the Contract will be considered the Processor and all other members of the BM Group involved in the Personal Data Processing on behalf of the Controller will be considered sub-processors for the purposes of this DPA.
Nature of Processing of Personal Data	Personal Data are Processed to provide the Services under the Contract in accordance with its terms, including the operations described in Art. 4 no. 2 GDPR. The respective roles and responsibilities of the members of the BM Group with respect to the provision of the Services, are described in the following Section "Roles and Responsibilities / Sub-processors".
Roles and Responsibilities / Sub-processors	**Intra-Group Sub-processing** The following members of the BM Group will act either as Processor or sub-processor as identified in Section "Subject-matter of Processing of Personal Data" hereinabove: **BuildingMinds Technology AG** Role: BuildingMinds Technology AG, Seestrasse 55, 6052 Hergiswil (NW), Switzerland is the central contracting hub of the BM Group for non-US Customers. BuildingMinds Technology AG either only enters into any framework agreements, which provide a general framework for individual Contracts, with non-US Customers, or (also) into the actual individual Contracts with non-US Customers. BuildingMinds Technology AG will have

access to all Personal Data Processed on behalf of Customers that entered into individual Contracts with BuildingMinds Technology AG.

For more information on processing activities and third-party sub-processors see our separate summary “How We Process Personal Data“ in its most current version available at the time of conclusion of the DPA at:

https://buildingminds.com/personal-data-processing

BuildingMinds GmbH

Role: BuildingMinds GmbH, Schindler-Platz, 12105 Berlin, Germany is the central technical and operational hub of the BM Group. BuildingMinds GmbH operates the BuildingMinds Platform and provides all Services, whether directly as a Contractor or as a sub-contractor of other BM Group entities. BuildingMinds GmbH therefore has access to all Personal Data Processed on behalf of the Controller within the BM Group and Processes such Personal Data for the provision of the Services.

For more information on processing activities and third-party sub-processors see our separate summary “How We Process Personal Data“ in its most current version available at the time of conclusion of the DPA at:

https://buildingminds.com/personal-data-processing

BuildingMinds, Inc.

Role: BuildingMinds, Inc., C/O Schindler Elevator Corporation, 1133 6th Avenue, 28th Floor, New York, New York 10036, USA is the central contracting hub of the BM Group for US Customers. BuildingMinds, Inc. enters into any framework agreements, which provide a general framework for individual Contracts, with US Customers, and (also) into any actual individual Contracts with US Customers. BuildingMinds, Inc. will have access to all Personal Data Processed on behalf of Customers that entered into individual Contracts with BuildingMinds, Inc.

For more information on processing activities and third-party sub-processors see our separate summary “How We Process Personal Data“ in its most current version available at the time of conclusion of the DPA at:

https://buildingminds.com/personal-data-processing

Hosting of the BuildingMinds Platform

The BuildingMinds Platform is hosted in the Microsoft Azure European cloud.

For more information on processing activities and third-party sub-processors see our separate summary “How We Process Personal Data“ in its most current version available at the time of conclusion of the DPA at:

https://buildingminds.com/personal-data-processing

Future Changes

The Controller will be informed of any intended addition or replacement of sub-processors covered in this **Appendix 1** in accordance with Section 8 of the DPA. The Controller may inform itself of future changes of the Processing activities and sub-processors of the individual entities listed above by regularly visiting the webpages

	linked above. The Controller will have the opportunity to object to any relevant changes in accordance with the terms of the DPA.
Types of Personal Data	Data relating to individuals and provided to the Processor by the Controller or persons authorized by the Controller through the use of Services under the Contract. Such data may e.g. include: name, age, birth date and place as well as other identification items used in contracts, usage habits and energy or other consumption data of real estate property users, private and professional contact information (e.g. phone and fax numbers, e-mail address, postal address), bank and / or invoice information, data bank and calendar entries, user name, system access, system preferences, system authorization, IP address, time zone, language and company name.
Purpose of Processing of Personal Data	Provision of Services under the Contract in accordance with its terms.
Categories of Data Subjects the Personal Data relates to	Individuals with respect to whom data is provided to the Processor by the Controller or persons authorized by the Controller through the use of Services under the Contract. Such individuals may e.g. include: the Controller, its suppliers, service providers or other contract partners, their respective employees and other individuals, such as users of the real estate properties of the Controller.
Duration of Processing of Personal Data	The term of the Contract and the period of time from the Contract expiry until deletion of the Personal Data by the Processor in accordance with the Contract terms.

Appendix 2 to the DPA

Technical and Organizational Measures:

Processor's administrative, physical, organizational and technical measures shall include, at a minimum, the following:

I. Pseudonymization and Encryption

The Processor takes the following measures to ensure pseudonymization, if necessary:

- *Commonly used pseudonymization measures help to replace name and other identification attributes with the aid of identifiers. The purpose of this is to prevent or make it considerably more difficult to identify the person concerned (the Data Subject).*
- *With the aid of various indicators, such as personnel, client or customer codes, pseudonymization is implemented. Accordingly, no real names are used.*

Controller's Personal Data is protected with the aid of encryption techniques. Where Personal Data is transmitted within a network, i.e. between user devices and data centers or within the data centers themselves, a minimum TLS version of 1.2 is used. To protect Personal Data in the state of rest, a range of integrated encryption functions are offered. The following methods are used in this connection:

- *Symmetric encryption: With the aid of a key, information is encrypted and decrypted.*
- *Asymmetric encryption: With the aid of two keys, namely public and private keys, information is encrypted and decrypted.*

II. Confidentiality

Strict measures are taken to protect the Controller's Personal Data from unlawful access or use by unauthorized persons. For this purpose, employee access is restricted.

1. Access Control of Persons

The Processor takes the following protective measures to prevent unauthorized persons from entering data processing facilities where Personal Data is processed or used:

- ***Physical Protection:***
  Access to physical data center facilities is protected by external and internal fencing. The security guidelines are extended as the level increases. This is achieved by the deployment of security personnel and by locked server racks. In addition, multifactorial access controls are carried out. An integrated alarm system and a 24/7 video surveillance provide further protection against unauthorized persons.

- ***Virtual protection:***
  Role-based access control, multifactor authentication and the minimization of constant access to production data purposefully restrict the system. Access to the Controller's Personal Data is fully logged. In order to ensure that this is properly implemented, regular audits (as well as random audits) are carried out.

2. System Access Control

The Processor takes the following measures to protect Personal Data Processing systems from use by unauthorized persons:

- *Personal Data is stored exclusively in secure data centers (see item 1 Access Control of Persons).*
- *The system access to all Personal Data Processing systems is routed via an SSL encrypted access.*
- *Personal Data cached on mobile data carriers is encrypted.*
- *System access to Personal Data Processing systems requires a special personal authorization. A password and a second authentication factor are required for this purpose.*
- *Employees leaving the company will have their system access cancelled within 24 hours of their leaving.*

3. **Data Access Control**

   The Processor takes measures to procure that the persons authorized to use a Personal Data Processing system can only access Personal Data within the scope of their access authorization. Measures are taken preventing that Personal Data can be read, copied, altered or removed without authorization during the Processing, use and after storage of the same. During the entire contractual term, the Controller has the possibility of accessing, extracting and erasing its data stored in the BuildingMinds Platform or request the Processor to do so.

   - *Only authorized employees, according to their respective role and necessity, may be given access to Personal Data. By these means, the Processor procures that employees involved in the processing of the Controller's Personal Data only process the same upon the instructions of the Controller. In addition, these persons are obliged to maintain confidentiality and security of Personal Data, also following the end of their employment.*
   - *All authorized persons require a special personal authorization. This authentication requires a password and a second authentication factor. The authenticated user can only access Personal Data in accordance with the assigned role.*
   - *The access of employees who have left the company is blocked upon the effective date of their departure.*
   - *Access can only be granted by administrators. The number of administrators is limited to the level necessary for the operation of the Personal Data Processing systems.*
   - *Compliance with password guidelines is ensured by the system technology and all logins are recorded in the system.*
   - *Authentication mechanisms based on passwords must be renewed regularly.*

4. **Order Control**

   The Processor implements the following measures to procure that Personal Data can only be Processed in accordance with the instructions of the Controller:

   - *Personal Data will only be used for the purposes defined in the Contract.*
   - *As between the Parties, the Controller reserves all rights, ownership and interest in its Personal Data. No rights to the Controller's Personal Data are provided, with the exception of the rights granted by the Controller.*

5. **Separation control**

   The Processor implements the following measures to procure that the Personal Data of different customers can be Processed separately:

   - *The data of individual tenants / customers is explicitly assigned to a customer. Data is marked with a unique customer ID and stored separately in the system.*
   - *Access to the data always requires a customer ID. The system limits access to this specific customer.*

III. Integrity

1. Monitoring of Data Transfer

The Processor takes the following measures to procure that Personal Data cannot be read, copied altered or removed by unauthorized persons in the course of electronic transmission, during its transport and during its storage on data carriers:

- *The Personal Data collected is protected at various levels.*
- *Cached Personal data is encrypted (see item I Pseudonymization and Encryption).*
- *Controller's Personal Data will not be disclosed to government agencies unless required by law. In the event of a request for the Controller's Personal Data by a law enforcement agency, the Processor will ask it to request the data directly from the Controller. If such request is enforced, the Controller will be informed without undue delay, unless prohibited by law.*
- *Following receipt of any requests for the Controller's Personal Data by other third parties, the Controller will be informed without undue delay, unless prohibited by law.*

2. Input Control

The Processor takes the following measures to ensure that it is possible to check and verify retrospectively whether and by whom Personal Data has been entered, altered or removed in data processing systems:

- *User accounts are assigned to individual users and cannot be split between several different users.*
- *Only certain system administrators have access to the information stored in the system, unless the creator of the file or the team that shares the document has granted write or read access.*
- *The system logs details of who last accessed Personal Data.*

IV. Availability and Resilience

1. Availability control

The Processor procures that the technical infrastructure provides high availability and reliability. With regard to this, the Processor takes the following measures for protecting Personal Data against accidental destruction or loss:

- *Interruption-free power supplies avoid unplanned system crash in the event of short-term power failures. In addition, emergency generators are used to take over the power supply in the case of longer power failures.*
- *High-speed and robust optic fiber networks connect data centers with other large hubs and Internet users.*
- *In addition, high availability is addressed through monitoring measures and the resulting rapid response to incidents.*
- *Geographically dispersed operations centers are in operation around the clock.*
- *Intelligent back-up failover capabilities cater for availability.*
- *Data is permanently held in two locations. Back-up site locations can be selected. This allows that flawless replicas can be created.*

2. Restorability

The Processor takes the following measures procuring that the systems used can be restored in the event of a breakdown:

- *Regular restore points are stored so that Personal Data can be restored.*

- *If a drive has a hardware fault, it is safely erased or destroyed before it is returned to the manufacturer for replacement or repair.*

V. Procedures for Periodic Review, Assessment and Evaluation

The Processor takes the following measures for periodic review, assessment and evaluation:

A data protection management is set up for a regular review of the technical and organizational measures implemented so that these can be adapted, where necessary.