Data Processing Appendix

1. Processing Operations and Definitions

(1) This Data Processing Appendix ("**DPA**") applies to all Processing operations regarding Personal Data and whenever Schindler ("**Processor**"), his employees or sub-contractors (as applicable) may come into contact with Personal Data Processed by the Processor on behalf of the Customer ("**Controller**") as part of the provision of services under the Contract. This shall include in particular, but not be limited to, the subject-matter and duration, the nature and purposes of Processing, the types of Personal Data and the categories of Data Subjects listed in **Exhibit 1** to this DPA.

(2) All capitalized terms used in this DPA which are defined in the General Data Protection Regulation (EU 2016/679 – "**GDPR**"), but not defined in this DPA or elsewhere in the Contract shall have the meaning as defined in the GDPR.

2. Processing on Behalf of the Controller

(1) The Processor shall Process Personal Data only within the scope of the Contract on the Controller's documented instructions. This shall not apply to backup copies where these are required to ensure proper Processing, or to any Personal Data required by the Processor to comply with statutory obligations.

(2) The Controller's instructions are defined in the other parts of the Contract. The Controller is not entitled to issue additional instructions, unless the Processor is able to carry out such instruction without unreasonable efforts and the Controller pays compensation for these additional efforts according to the Processor's then current rates on a time and material basis.

(3) 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.

(4) If the Processor considers an instruction to violate applicable data protection laws, he shall inform the Controller immediately and be entitled to suspend the execution of the relevant instructions until the Controller confirms or changes them.

3. Obligations of the Processor

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

(2) The Processor shall correct, delete or block Personal Data in the scope of this DPA where the Controller issues such instruction or, where the Controller so instructs, return such data to the Controller upon compensation of Processor's reasonable costs, calculated on time and material basis, unless and for as long as applicable law requires storage of the Personal Data.

(3) The Processor's personnel engaged in performing Processing operations under this DPA have been bound to confidentiality or are 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 the internal processes and the technical and organizational measures to ensure that Processing within his area of responsibility is in accordance with the applicable data protection laws.

(6) The Processor shall reasonably assist the Controller at the Controller's expense (according to the then current rates of the Processor on a time and material basis) in complying with his obligations according to Art. 32 to 36 GDPR.

(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 seq. GDPR have been fulfilled. For that purpose, the Processor may enter – if necessary, as agent for and on behalf of the Controller – into standard data protection clauses adopted by the Commission under EU Directive 95/46/EC or the GDPR ("**SCC**") with any sub-processors established in third countries (not ensuring an adequate level of data protection) and engaged in the Processing of Personal Data under this DPA. Such SCC may be supplemented as necessary to meet the requirements of applicable data protection laws, including Art. 28(3) GDPR, as long as such supplements do not contradict the Contract (including the DPA) and the SCC in their original form. The Processor is entitled to exercise Controller's instruction and control rights under SCC entered on behalf of Controller. Sub-processors that have entered into SCC with Controller will be third party beneficiaries of Sec. 8(1) and Sec. 10 of this DPA.

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, and where the Controller reimburses the Processor for the cost and expenses (according to the then current rates of the Processor on a time and material basis) incurred in providing such support. 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 are brought by the Data Subject against the Processor, the Controller undertakes to reasonably assist the Processor's defence against such claims.

6. Technical and Organizational Measures

(1) The Processor will implement and maintain the technical and organizational measures set out in **Exhibit 2** to this DPA.
(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 if the Processor becomes aware of any Personal Data breach of the Controller. 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. Subcontracting

(1) The Processor may not subcontract any or a portion of the Processing of Personal Data to sub-processors without the Controller's prior consent. The Controller hereby consents to the Processor engaging sub-processors in the Processing of Personal Data on behalf of the Controller, including those sub-processors listed in **Exhibit 3** to this DPA. If Controller has entered into any SCC as described in Sec. 3(7) above, the above consent constitutes Controller's prior written consent to the subcontracting of the Processing of Personal Data on behalf of the Controller under such SCC.
(2) The Processor shall notify the Controller about any substitution of or addition to the sub-processors. The Controller shall promptly inform the Processor in writing within ten (10) days as of the receipt of the Processor's notification, if and on which reasonable grounds he objects to the substitute or additional sub-processor. Otherwise, the Controller will be deemed to have consented to such substitution or addition.
If the Controller objects to a substitute or additional sub-contractor in time, 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 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, the Controller may terminate the DPA by providing written notice to the Processor.
In case of a termination of the DPA by the Processor or the Controller in accordance with this paragraph the entire Contract shall terminate concurrently.
(3) 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 in its reasonable discretion believes that the rights under paragraph 1 are not sufficient in an individual case, or a competent data protection authority requests an audit. The audit will 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 set up.
(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) month 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 may claim remuneration for its efforts when enabling the Controller's audits according to the then current rates of the Processor on a time and material basis.
(5) The Processor is under no obligation to disclose or provide access to any (i) data related to other customers of (x) 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 premises of the Processor's, its affiliates or any sub-processors.

10. Liability and Damages

The liability provisions as agreed between the parties in the Contract apply accordingly to any liability arising out of or in connection with any SCC entered into on behalf of the Controller in accordance with Sec. 3(7) above. Damages

recovered by a party to the Contract (including this DPA) or any SCC thereunder is counted towards corresponding damage claims of such party under any of the other aforementioned agreements.

11. Miscellaneous

In case of any contradictions, the provisions of this DPA shall take precedence over the other provisions of the Contract.

EXHIBIT 1 TO THE DPA
CERTAIN PERSONAL DATA- AND PROCESSING-RELATED INFORMATION

Subject-matter of Processing of Personal Data	Provision of services to Controller under the Contract.
Nature of Processing of Personal Data	Personal Data Processing to provide services under the Contract in accordance with its terms, including the operations described in Art. 4 no. 2 GDPR.
Types of Personal Data	Data relating to individuals and provided to Processor by Controller or persons authorized by Controller through the use of services under the Contract. Such data may e.g. include: name, phone and fax numbers, e-mail address, postal address, user ID, system access / usage / authorization, time zone, language, company name and other legal entity information.
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 Processor by Controller or persons authorized by Controller through the use of services under the Contract. Such individuals may e.g. include: Controller, its employees, contract partners and other individuals.
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 Processor in accordance with the Contract terms.

EXHIBIT 2 TO THE DPA
TECHNICAL AND ORGANIZATIONAL MEASURES

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

1. Confidentiality

- Physical Access Control
  Processor maintains physical access control standards designed to restrict unauthorized physical access to data storage and processing facilities. Entry points are controlled by electronical and mechanical locks. Furthermore, facility security services are in place. Processor's internal regulations ensure that upon termination of employment, access authorizations of employees are revoked and access badges and/or keys are returned.
- Electronic Access Control
  Electronic access to all data storage and processing systems are protected with a secure password. Password expiration and strength (minimum of 10 alphanumeric characters) are governed by Processor's internal regulations. Access from outside the Processor network is provided only via Virtual Private Networks (VPN), using a two-factor authentication. Tokens granted for remote access are revoked when the access is not necessary anymore.
- Internal Access Control
  For all data processing and storage systems a need-based authorization concept and mechanism to prevent unauthorized access to Personal Data has been implemented. Access authorizations are subject to regular validation as outlined in Processor's internal regulations.

2. Integrity

- Data Transfer Control
  All Personal Data transferred from any equipment collecting such data to the Processor systems is encrypted and transferred via a secured channel.
- Data Entry Control
  Processor logs and monitors whether and by whom Personal Data is entered into data storage and processing systems, when changed or deleted.

3. Availability and Resilience

- Availability Control
  All Personal Data is subject to a backup. Back-up copies of information and software are taken and tested regularly in accordance with the Processor's internal regulations.
- Rapid Recovery
  Data recovery procedures for the different data storage and processing systems are in place and are regularly revalidated. The procedures and measures to ensure business continuity are laid out in Processor's internal regulations. Regular checks on business continuity are conducted. Sub-processors that handle data on behalf of Processor are certified by a third party to guarantee for full redundancy and maximum uptime.

4. Procedures for Regular Testing, Assessment and Evaluation

- Data Protection Management
  Procedures for incident, change and test management, including automatic test procedures, are in place and are regularly revalidated. Additional security and safety-related testing is done at specific quality gates during the application development process by the Processor's Cyber Security Department as well as by third parties on demand. Upon deployment and each change, applications are scanned for the differing scope.

5. Data Protection by Design and Default
   To ensure that systems are designed for data protection compliance and security, all security requirements are identified and documented during the design phase of a project, in accordance with Processor's internal regulations.

6. Order and Sub-processor Control

- Order Control
  Personal Data Processing is performed only within the scope of the Contract and on the Controller's documented instructions. Controller's complete and final instructions for the Processing of Personal Data are defined by Controller's and its authorized users' use of services under the Contract.
- Sub-processor Control
  Processor will engage a third party in the Processing of Personal Data only upon Controller's prior consent and on the basis of clear contractual arrangements with respect to appropriate security, confidentiality and privacy.

EXHIBIT 3 TO THE DPA
LIST OF SUB-PROCESSORS

The Controller consents to the Processor engaging the following sub-processors:

Subprocessor	**Address**	**Description of services provided by the sub-processors**
Schindler Digital Group AG	Zugerstrasse 13, 6030 Ebikon, Switzerland	Management of Personal Data
Schindler IT Services AG	Zugerstrasse 13, 6030 Ebikon, Switzerland	Management of Personal Data
Schindler Digital Business GmbH	Schindler-Platz, 12105 Berlin, Germany	Management of Personal Data