Data Processing Agreement
under Articles 28 and 29 of Regulation (EU) 2016/679

between

Controller
Tbd

subsequently called the "**Controller**"
and

1. PlanRadar GmbH
FN 400573 d
Schottenring 16, DG 1
1010 Vienna
Austria

and

2. PlanRadar Singapore Pte. Ltd.
10 Anson Road
#29-07 International Plaza
Singapore 079903

collectively called the "**Processors**" or "**Joint Processors**", each individually called the "**Processor**", and together with the Controller referred to as the "**Parties**".

1. Purpose and scope

(a) The purpose of these standard contractual clauses (the "**Clauses**") in this data processing agreement (the "**Agreement**") is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, the Personal Data Protection Act 2012 of Singapore ("**PDPA**"), and any other applicable data protection laws, rules, and regulations.

(b) The Controller(s) and Processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679, the PDPA, and any other applicable data protection laws, rules, and regulations.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the Controller is subject by virtue of Regulation (EU) 2016/679, the PDPA, and any other applicable data protection laws, rules, and regulations.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679.

2. Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

3. Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 respectively, those terms shall have the same meaning as in that Regulation, unless stated otherwise.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679, the PDPA, and any other applicable data protection laws, rules, and regulations respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679, the PDPA, and any other applicable data protection laws, rules, and regulations, or in a way that prejudices the fundamental rights or freedoms of the data subjects.

4. Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

In case of any inconsistency between the provision(s) of any data protection laws, rules, and regulations, including but not limited to Regulation (EU) 2016/679 and the PDPA, the provision(s) offering a higher standard of protection shall prevail to the extent of such inconsistency.

5. Docking clause

(a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a Controller or a Processor by completing the Annexes and signing Annex I.

(b) Once the Annexes in Clause 5(a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a Controller or a Processor, in accordance with its designation in Annex I.

(c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

6. Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the Controller, are specified in Annex II.

7.Obligations of the Parties

7.1. Instructions

(a) The Joint Processors shall process personal data only on documented instructions from the Controller, unless required to do so by Union or Member State law or the PDPA to which any of the Processor is subject. In this case, each Processor shall inform the Controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the Controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The Joint Processors shall immediately inform the Controller if, in either Processor's opinion, instructions given by the Controller infringe the PDPA, Regulation (EU) 2016/679, the applicable Union or Member State data protection provisions, and/or any other applicable data protection laws, rules, and regulations.

7.2. Purpose limitation

The Joint Processors shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the Controller.

7.3. Duration of the processing of personal data

Processing by the Joint Processors shall only take place for the duration specified in Annex II.

7.4. Security of processing (Section 24 of the PDPA)

(a) The Joint Processors shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects. For the avoidance of doubt, the Processors and the Controller shall each comply with all their respective obligations under (1) Regulation (EU)

2016/679, (2) the PDPA, and/or (3) any other applicable data protection laws, rules and regulations at their own cost, [but the Processors may share such costs between themselves as they deem fit in their sole discretion].

(b) The Joint Processors shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. Each Processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("**sensitive data**"), the Joint Processors shall apply specific restrictions and/or additional safeguards as they deem necessary in compliance with all data protection laws which apply to them.

7.6 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The Joint Processors shall deal promptly and adequately with inquiries from the Controller about the processing of data in accordance with these Clauses.

(c) The Joint Processors shall make available to the Controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679, the PDPA, and/or any other applicable data protection laws, rules, and regulations. At the Controller's request, the Joint Processors shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the Controller may take into account relevant certifications held by the Joint Processors.

(d) The Controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the Joint Processors and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

(f) Where the Controller provides any personal data of the data subjects to either or both Processors, the Controller shall make reasonable effort to ensure that such personal data is accurate and complete before providing the same to either or both Processors. If there is any error in any such personal data provided by the Controller to either or both Processors, the Controller shall take steps to inform either or both Processors as soon as reasonably practicable in writing such that

either or both Processors are able to correct any such error as soon as reasonably practicable.

7.7. Use of sub-processors

(a) Neither Processor shall subcontract any of its processing operations performed on behalf of the Controller in accordance with these Clauses to a sub-processor, without the Controller's prior specific written authorisation. The Processors shall submit the request for specific authorisation at least 4 weeks prior to the engagement of the sub-processor in question, together with the information necessary to enable the Controller to decide on the authorisation. The list of sub-processors authorised by the Controller can be found in Annex IV. The Parties shall keep Annex IV up to date as far as is reasonably practicable.

(b) Where either Processor engages a sub-processor for carrying out specific processing activities (on behalf of the Controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the Processors in accordance with these Clauses. Each Processor shall ensure that the sub-processor complies with the obligations to which either Processor is subject pursuant to (1) these Clauses, (2) Regulation (EU) 2016/679, (3) the PDPA, and/or (4) any other applicable data protection laws, rules and regulations. In case of any inconsistency between the provision(s) of any such data protection laws, rules, and regulations, the provision(s) offering a higher standard of protection shall prevail to the extent of such inconsistency.

(c) At the Controller's request, each Processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the Controller. To the extent necessary to protect business secret or other confidential information, including personal data, each Processor may redact the text of the agreement prior to sharing the copy.

(d) The Joint Processors shall remain fully responsible to the Controller for the performance of the sub-processor's obligations in accordance with its contract with the Processor. Each Processor shall notify the Controller of any failure by the sub-processor to fulfil its contractual obligations.

(e) The Joint Processors shall agree to include a third party beneficiary clause for the benefit of the Controller in either or both Processors' sub-processor agreement with the sub-processor, whereby in the event that either Processor or both Processors have factually disappeared, ceased to exist in law or has become insolvent, the Controller shall have the right to terminate the sub-processor agreement at its sole discretion and to instruct the sub-processor to erase or return any personal data so retained pursuant to such sub-processor agreement.

7.8. International transfers (Section 26 of the PDPA)

(a) Any transfer of data to a third country or an international organisation by the Joint Processors shall be done only on the basis of documented instructions from the Controller or in order to fulfil a specific requirement under Union or Member State law to which either Processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679, the PDPA, and/or any other applicable data protection laws, rules and regulations, and shall in any event, be

protected at a standard that is comparable to that under the PDPA pursuant to Section 26 of the PDPA. In case of any inconsistency between the provision(s) of any data protection laws, rules, and regulations, including but not limited to Regulation (EU) 2016/679 and the PDPA, the provision(s) offering a higher standard of protection shall prevail to the extent of such inconsistency.

(b) The Controller agrees that where either Processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the Controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the PDPA, and/or any other applicable data protection laws, rules, and regulations, the Processors and the sub-processor can ensure compliance with (1) Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the European Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679 and (2) the PDPA, provided the conditions for the use of those standard contractual clauses as well as the compliance with any other applicable data protection laws, rules, and regulations are met. In any event, such transfer of personal data shall be protected at a standard that is comparable to that under the PDPA pursuant to Section 26 of the PDPA. In case of any inconsistency between the provision(s) of any data protection laws, rules, and regulations, including but not limited to Regulation (EU) 2016/679 and the PDPA, the provision(s) offering a higher standard of protection shall prevail to the extent of such inconsistency.

8. Assistance to the Controller

(a) Each Processor shall promptly notify the Controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the Controller.

(b) Each Processor shall assist the Controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with Clauses 8(a) and 8(b), each Processor shall comply with the Controller's instructions as far as is reasonably practicable.

(c) In addition to the Processors' obligation to assist the Controller pursuant to Clause 8(b), the Processors shall furthermore assist the Controller as far as reasonably practicable in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the Processors, including but not limited to preventing unauthorised or accidental access, collection, use, disclosure, copying, modification, disposal or destruction of personal data of data subjects, or any other similar risks, as well as the loss of any storage medium or device on which such personal data is stored (where applicable) in accordance with Regulation (EU) 2016/679, Section 24 of the PDPA, and/or any other applicable data protection laws, rules, and regulations:

(1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the Controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the Controller without delay if the Processors become aware that the personal data it is processing is inaccurate or has become outdated; and

(4) the obligations in Article 32 Regulation (EU) 2016/679.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the Processors are required to assist the Controller in the application of this Clause as well as the scope and the extent of the assistance required. The Controller hereby agrees that it shall not unreasonably withhold its consent to either or both Processors amending any such technical and organisational measures if either or both Processors deem it necessary or desirable to do so, but in any event subject always to its/their compliance with all applicable data protection laws, rules, and regulations applying to either or both Processors.

9. Notification of personal data breach (Sections 26C and 26D of the PDPA)

In the event of a personal data breach, the Joint Processors shall cooperate with and assist the Controller for the Controller to comply with its obligations under Articles 33 and 34 Regulation (EU) 2016/679, Sections 26C and 26D of the PDPA, and/or any other applicable data protection laws, rules, and regulations where applicable, taking into account the nature of processing and the information available to the Processors.

9.1 Data breach concerning data processed by the Controller

In the event of a personal data breach concerning data processed by the Controller, the Joint Processors shall assist the Controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the Controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) Regulation (EU) 2016/679, Section 26D(3) of the PDPA, and/or Regulation 5 of the Personal Data Protection (Notification of Data Breaches) Regulations 2021, shall be stated in the Controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach; and

(3) the measures taken or proposed to be taken by the Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to Article 34 Regulation (EU) 2016/679 and/or Section 26D(2) of the PDPA with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the Joint Processors

In the event of a personal data breach concerning data processed by the Joint Processors, each Processor shall notify the Controller without undue delay after either Processor having become aware of the breach in accordance with Section 26C(3) of the PDPA and/or any other applicable data protection laws, rules, and regulations. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained; and

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay. The Controller shall, upon such notification by either or both Processors, conduct an assessment of whether such personal data breach is a breach notifiable to the Personal Data Protection Commission of Singapore ("**SG Commission**"), and if so, notify the (1) SG Commission as soon as is reasonably practicable (but in any case no later than three calendar days after the Controller has made such assessment) and (2) each affected individual whose personal data has been breached in a manner that is reasonable in the circumstances in accordance with Section 26D of the PDPA.

The Parties shall set out in Annex III all other elements to be provided by the Joint Processors when assisting the Controller in the compliance with the Controller's obligations under (1) Articles 33 and 34 of Regulation (EU) 2016/679, (2) Section 25 of the PDPA, and/or (3) any other applicable data protection laws, rules, and regulations, including but not limited to the Processors not retaining personal data of the data subjects (or any documents or records containing such personal data, electronic or otherwise) for any period of time longer than is necessary to serve the purposes of this Agreement.

SECTION III – FINAL PROVISIONS

10. Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679, Regulation (EU) 2018/1725 and/or any other applicable data protection laws, rules, and regulations, in the event that the Joint Processors are in breach of its obligations under these Clauses, the Controller may instruct either Processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. Each Processor shall promptly inform the Controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The Controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by either Processor has been suspended by the Controller pursuant to Clause 10(a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) either Processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679, Regulation (EU) 2018/1725, and/or any other applicable data protection laws, rules, and regulations; and

(3) either Processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679, Regulation (EU) 2018/1725, and/or any other applicable data protection laws, rules, and regulations.

(c) Each Processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the Controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the Controller insists on compliance with such instructions.

(d) Following termination of the contract, the Joint Processors shall, at the choice of the Controller, delete all personal data processed on behalf of the Controller and certify to the Controller that it has done so, or, return all the personal data to the Controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, each Processor shall continue to ensure compliance with these Clauses.

SECTION IV – MISCELLANEOUS

11. Governing law and dispute

(a) This Agreement and the implementation and interpretation of it are governed by and subject to the laws of Singapore. If there occurs any dispute or controversy between the Parties concerning or in relation to this Agreement and/or any matter dealt with in or relating to this Agreement and/or the performance and/or interpretation of this Agreement, the Parties shall endeavor to settle such dispute or controversy amicably.

(b) If the dispute or controversy cannot be settled amicably by the Parties within 30 calendar days after the matter being disputed is conveyed by to the other Party

by a Party raising the dispute or controversy, either Party or the Parties together may submit the dispute or controversy to arbitration for the exclusive and final settlement of such dispute or controversy.

(c) Any dispute arising out of or in connection with this Agreement, including any question regarding its existence, validity or termination, shall be referred to and finally resolved by arbitration administered by the Singapore International Arbitration Centre in accordance with the Arbitration Rules of the Singapore International Arbitration Centre for the time being in force, which rules are deemed to be incorporated by reference in this Clause. The seat of the arbitration shall be Singapore. The governing law of arbitration shall be Singapore law. The Tribunal shall consist of one arbitrator. The language of the arbitration shall be English. The decision of the arbitration tribunal shall be final and binding on the Parties.

12. Notices

(a) (1) All notices, demands or other communications required or permitted to be given or made by the Parties under this Agreement, unless stated otherwise, shall be in writing and delivered personally or sent by registered post addressed to the intended recipient thereof or by electronic mail at their electronic mail address set out below (or to such other address or electronic mail address as the relevant Party may from time to time notify the other):

To the Controller:

[**]**

Address	:	
Contact/Department	:	
Email	:	

To the Processor:

PlanRadar GmbH

Address	:	FN 400573 d Kärntner Ring 5-7 1010 Vienna Austria
Contact/Department	:	
Email	:	

To the Processor:

PlanRadar Singapore Pte. Ltd.

Address	:	10 Anson Road #29-07 International Plaza Singapore 079903
Contact/Department	:	

Email :

(2) Any notice, demand, or communication sent pursuant to this Clause shall be deemed to have been duly served (if given by electronic mail) at the time the electronic mail containing the notice left the sender's electronic mail system, unless the sender receives notification that the electronic mail containing the notice was not received by the recipient, or (if given or made by facsimile) immediately, or (if given or made by registered post) seven (7) calendar days after posting or after it has been sent by first class courier and in proving the same it shall be sufficient to show that the envelope containing the same was duly addressed, stamped and posted by certified or registered mail or sent by courier.

(3) Rejection, other refusal to accept or inability to deliver any communication because of any change in details of either Party in its address, telephone number, fax number, email address and/or substitute address of which such change was not promptly notified in writing from either Party to the other Party shall be deemed to be duly served on the other Party under this Agreement.

(b) To the fullest extent permitted by law, the Parties agree that any originating process and any document for any claim, legal action or arbitration proceeding may be served in the manner set out in this Clause.

13. Severability

If any provision of this Agreement or any part thereof is declared to be invalid, illegal, unenforceable, in conflict with any applicable laws, rules, and regulations, or contrary to public policy pursuant to any applicable laws, rules, and regulations, such invalidity, illegality, unenforceability, conflict, or contravention shall attach only to such provision or part thereof, whereas the validity, legality, and enforceability of the remaining part of such provision and all other provisions of this Agreement shall not in any way be affected or impaired and shall therefore remain in full force and effect. In any such event, the Parties shall where applicable, execute such documents as to give valid, legal, or enforceable effect to the invalid, illegal, unenforceable, conflicting, or contravening provision or part thereof, or to effect new provision or provisions which shall restore this Agreement as nearly as possible to what the Parties intended by the original provision and the purpose thereof.

Vienna, date _____ **Place, date** _____

For PlanRadar GmbH

and PlanRadar Singapore Pte. Ltd.

For Controller

ANNEX I LIST OF PARTIES

Controller(s):

1. Name: _____

   Address: _____

   Name and contact data of the data protection officer:_____

Processor(s):

1. PlanRadar GmbH
   FN 400573 d
   Kärtner Ring 5-7
   1010 Vienna
   Austria

2. PlanRadar Singapore Pte. Ltd.

   10 Anson Road

   #29-07 International Plaza

   Singapore 079903

Name and contact data of the data protection officer: Constantin Köck, c.koeck@planradar.com

Vienna, date _____ **Place, date _____**

For PlanRadar GmbH and PlanRadar Singapore Pte. Ltd.	**For Controller**

ANNEX II: DESCRIPTION OF THE PROCESSING

Categories of data subjects whose personal data is processed

- The users of the PlanRadar software-as-a-service solution, who have been invited to the projects by the Controller (e.g. customers, subcontractors, employees)

Categories of personal data processed

- Communication data (e-mail address, optional telephone number)
- Contract data (name, e-mail, company)
- Ticket information (creator, creation date, modification date, voice memo)

Nature of the processing

- Depending on the user's needs, the processing includes the collection, recording, organisation, classification, storage, adaptation or alteration, retrieval, consultation, use, transmission, alignment or combination, restriction, or deletion of data.

Purpose(s) for which the personal data is processed on behalf of the controller

- To provide the PlanRadar software-as-a-service solution for construction documentation, task and defect management, in particular to simplify documentation and communication in construction and real estate projects. For this purpose, the user can process data on projects, tasks, individual work steps and the respective persons involved via the cloud-based software.

Duration of the processing

- The duration of the processing shall be governed by the main contract. In addition, the controller may terminate the contract in accordance with clause 10.

For processing by (sub-)processors:

- The storage of data in the cloud (Cloud Hosting) is carried out by sub-processor (see Annex IV). The duration of the processing depends on the main contract.

ANNEX III - TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

A. Entrance control

The aim is to protect access to data processing facilities where personal data is processed or used from unauthorized individuals.

Measure	Description
Alarm systems	The alarm systems for securing a building against break-ins and other criminal activities are in place. In the event of an alarm-triggering incident, an immediate notification is sent to a central security center.
Data centers*	The data centers, servers, and host software systems are locked in unassuming buildings. They are secured through physical security measures to prevent unauthorized access, both outside the premises (via fences and walls) and within the buildings.
Alarm systems at server locations*	Access to server locations is secured by alarm systems that trigger an alert when the door is compromised.
Automatic access control at server locations*	Access to server locations is managed through electronic access controls that trigger an alarm if the door is tampered with or held open.
Chip cards and expense control	Security against unauthorized entry is maintained with chip cards. An official chip card handover sheet must be signed by every employee. Chip cards must not be given to other persons.
Visitor record	Visitors must always identify themselves, and they are always accompanied by the employees.
Visitor record at server locations*	Visitors are required to identify themselves and go through the registration process, and they are continuously accompanied by authorized personnel. Access authorization is granted by an authorized person and revoked within 24 hours after an employee or supplier record has been deactivated.
Porter/guard	Porter and security services monitor access to the building.

Porter/guard at server locations *	Porter and security services monitor access to the building and sensitive areas. Trained security personnel guard the data centers and the surrounding area 24/7.
Video surveillance	Video monitoring has been implemented throughout the building to oversee access control.
Video surveillance at server locations *	Access to sensitive areas at data centers is monitored through video surveillance.

B. Access control

The goal is to prevent unauthorized individuals from using data processing systems.

Measure	**Description**
User rights at data centers*	Each user is provided with a unique ID to ensure that all system components can only be accessed by authorized users and administrators. The creation, deletion, and modification of user IDs, login credentials, and other identification features are logged along with a timestamp.
User profiles	User accounts are initially provisioned with the least access rights; periodic reviews of assigned permissions, especially for administrative user accounts, are conducted.
User profiles at data centers*	User access is only enabled once the HR department creates a corresponding record in the HR system. The principle of least privilege on a 'need-to-know' basis is followed. The granted access rights to IT systems are subject to quarterly review by authorized personnel. Access permissions are promptly revoked when they are no longer necessary for the user's tasks.
Password assignment	Passwords/passphrases for initial login are comprised of a unique value and must be changed immediately after the first use.

Authentication	Authentication is secured by username and password. In addition, multi-factor authentication has been introduced, which is based on at least two of the following factors (PIN codes or biometric features).
Password-Policy	Security measures include the implementation of automatic account lockouts after repeated failed login attempts and the activation of two-factor authentication for particularly important accounts.
Password-Policy at data centers*	User passwords must be changed at least every 90 days. Only complex passwords are allowed. Changing the password through simple password variations, such as altering a single character, is not permitted.
Clean-Desk/Clear-Screen-Policy	All employees are instructed to store all documents and materials in lockable cabinets or drawers when leaving their workplace. Automatic locking mechanisms for computers/laptops/notebooks when leaving the workspace or during periods of inactivity. Paper documents containing confidential information are shredded or properly disposed of. Chip cards and other physical access methods are securely stored and not openly visible.
WLAN policy	Visitors may only use the dedicated guest-WiFi. Employees must not reveal or give visitors access to the main WLAN-network.
Intrusion Detection/Intrusion Prevention System	Early attack detection, vulnerability identification, safeguarding critical resources, logging and reporting, as well as regular updates and maintenance, are all in place.
Firewalls	Hardware- and software firewalls are deployed and serve as essential elements to protect your network from unauthorized access, cyber threats, and potential security breaches.
Hardware firewall at data centers*	Antivirus software has been deployed, featuring both an email filter and malware detection capabilities.
Software firewall at data centers*	Firewall devices have been set up to limit access to the data processing environment and bolster the security of the computing clusters.

C. Admittance control

The intention is to ensure that authorized users of a data processing system can exclusively access data for which they have access permissions, and that personal data cannot be read, copied, altered, or removed without authorization during processing, use, and after storage.

Measure	Description
Anti-Virus-Software	Access control, ensuring protection against unauthorized system usage, is fortified by antivirus software. The software performs a daily check for updates.
Disk encryption	Protection against unauthorized system usage is ensured through the encryption of data storage devices.
Authorization concept	The principles of "Least Privilege," "Need-to-Know," and "Segregation of Duties" are upheld.
System administrator	Regular review of the granted permissions, particularly for administrative user accounts, is in place. The number of administrators is kept to the "essential" minimum. Unauthorized reading, copying, modification, or deletion within the system is strictly prohibited.
Access recording	Recording of all access; captures data such as the username, access timestamp, access type, and other relevant information.
Retention periods	The data retention periods are either legally mandated or established based on data protection regulations.

D. Input control

The purpose is to ensure that it can be retrospectively verified and determined whether and by whom personal data in data processing systems has been entered, modified, or removed.

Measure	Description
Processing register	The processing register has been created and is regularly reviewed.
Input, modification, and deletion of data	Recording the input, modification, and deletion of data, tamper-evident email archiving, retention of

	forms from which data has been transferred to automated processing, traceability of data input, modification, and deletion through individual usernames (not user groups).
Protocol and log files	The determination of whether and by whom personal data has been entered, altered, or removed from data processing systems. Log and protocol files are secured.

E. Disclosure control

The intention is to ensure that personal data cannot be read, copied, altered, or removed without authorization during electronic transmission or while stored on data carriers, and that, if necessary, it can be verified and determined.

Measure	**Description**
Pseudonymization	Identifiers are used, where possible, instead of names.
Dedicated lines or VPN tunnels	Access to production data is restricted to whitelisted IP addresses (access via Virtual Private Networks (VPN) or office network with dedicated line).
Prevention of unauthorized copying at data centers*	Employees are not allowed to connect personal electronic devices to information systems.
Data encryption	Unauthorized reading, copying, modification, or removal during electronic transmission or transport is prevented through the use of encryption. All data is encrypted, both during storage (Encryption at Rest) and during transmission (Encryption in Transit).
Deletion policy	Deletion deadlines, applied to both data itself and metadata like log files, are in place. The data remains available for download for 30 days after the termination of the main contract and is afterwards, if permitted by law, irrevocably deleted.
Recording the destruction process	Recording of destruction relates to documenting and recording of all processes that involve the disposal, deletion, or destruction of data.
Decommissioning of storage devices in the data centers*	When a storage device reaches the end of its lifespan, all retired magnetic storage devices are demagnetized

	and physically destroyed in accordance with industry standards and applicable data protection laws.

F. Order control

The goal is to ensure that personal data processed on behalf of data controller can only be processed in accordance with the instructions.

Measure	Description
Data confidentiality	Regular employee training is implemented to ensure standard processes during employee transitions or departures.
Written instructions	Clear contract formulation; no data processing takes place without clear instructions from the data controller as per Art. 28 GDPR.
Data destruction upon the termination of the contract	Deletion deadlines for both data itself and metadata like log files are in place. The destruction of data upon the termination of the contract is ensured.
Sub-processor	Strict selection of sub-processors (ISO certification, ISMS) and ensuring that the technical and organizational measures are also adhered to by the sub-processor through the data processing agreement.

G. Availability control

The purpose is to ensure that personal data is protected against accidental destruction or loss.

Measure	Description
Uninterruptible power supply (UPS) in data centers*	The electrical systems have been designed to ensure complete redundancy and can be maintained without affecting operations. The redundant data centers operate around the clock, seven days a week. Uninterruptible Power Supply (UPS) devices ensure continuous power supply for critical areas in the event of a power outage. Generators are also installed to provide emergency power to the entire facility when needed.

Air conditioning in the data centers*	Employees and relevant systems monitor the temperature and humidity in the data centers to ensure they are maintained at suitable levels.
Fire extinguishing equipment in data centers*	Automatic fire detection and suppression facilities are in place within the data centers. The fire detection system employs smoke sensors throughout all areas of the data centers, covering mechanical and electrical infrastructure, cooling rooms, and the spaces housing the generators.
Theft protection in data centers*	Secure placement of systems to ensure protection against theft.
Backup/Recovery	Protection against accidental or deliberate destruction or loss through backup strategy. The data is also secured through regular testing and recovery exercises. The backup and recovery concept are regularly reviewed and adapted to changing requirements and technologies.
Emergency plan	The regular review of the emergency plans takes place annually, ensuring integration of business continuity management.
Storage of data backups at offsite location*	The backup system is configured georedundantly, with backups stored in different buildings and different fire zones.
System landscape	The production systems are designed redundantly to maintain operations.
Penetration tests, testing, and release procedures	Software undergoes testing and release procedures to identify and fix errors, bugs, and vulnerabilities.
Protection against malware and patch management	Regular monitoring of security update and system vulnerability status, anti-malware software, and regular implementation of security patches and updates are in place.

H. Separation Control

The endeavor is to ensure that data collected for different purposes can be processed separately.

Measure	Description
Logical separation	Separate processing of data collected for different purposes: client capability, sandboxing.
Separation of production and test systems	Test and production systems are logically separated to reduce the risk of unauthorized access or unauthorized changes to the production systems.

I. Cryptography and Pseudonymization

The purpose is to ensure that information is protected from unauthorized access and remains unaltered during transmission or storage.

Measure	Description
Pseudonymization	If feasible for the specific data processing, the primary identifying characteristics of personal data are removed within the respective data application and stored separately.
Encryption of data storage devices and endpoints	The encryption of data storage devices (e.g., portable hard drives, USB sticks) and endpoints (PCs, laptops).

J. Data Protection Management

The aim is the appropriate assignment of central responsibilities to ensure control over the measures described above and maintain a high standard of security.

Measure	Description
Data Protection Officer	Data Protection Officer has been designated.
Data protection management	Employees are committed to confidentiality and the preservation of data secrecy, including regular employee training and awareness measures.
Privacy by design/default	The implementation of opt-out instead of opt-in and privacy by default/design is implemented to enhance user data privacy and security from the outset.
Certifications	ISO 27001 Certification, along with the Statement of Applicability, provides a framework for identifying,

	controlling, and reducing the risks associated with data security.
Internal audits	Security checks at the infrastructure and application levels are conducted regularly. Annual internal audit according to ISO 27001 is performed.
External audits	External audits are conducted as part of the ISO 27001 certification process.
Regular review	Procedures for reviewing, assessing, and evaluating technical and organizational measures are conducted regularly.
IT security	Incident response management, attack detection, monitoring and alerting, asset management, software management and distribution, user policies for device handling, and behavior in the use of information technology are implemented.

Annotation:

The marked (*) sections pertain exclusively to data centers of our sub-processor, Amazon Web Services, as the cloud hosting provider.

ANNEX IV: LIST OF SUB-PROCESSORS

EXPLANATORY NOTE:

The controller has authorised the use of the following sub-processors:

1. Amazon Webservices (Amazon Web Services EMEA SARL)
   38 Avenue John F. Kennedy, L-1855 Luxembourg

Description of the processing:

This sub-processor is used to store the data in the cloud (cloud hosting). The server location is in Frankfurt (AWS Region Europe (Frankfurt), eu-central-1). The storage of all data takes place within the European Union.