Data Processing Agreement

UK GDPR and EU GDPR

between

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

2. PlanRadar Limited
6th Floor 2 London Wall Place
EC2Y 5AU London
United Kingdom

collectively called as “Processors” or “Joint Processors”, each individually called as the “Processor”

and

[INSERT NAME / ORGANISATION]
[INSERT Address]
United Kingdom

subsequently called as the “Controller” and together with the Processors referred to as the “Parties” agreed upon following:

1. **DEFINITIONS**

1.1 In this Data Processing Agreement (referred to as “Agreement”, or “this Agreement”, or “our Agreement”), defined terms shall have the same meaning, and the following definitions have the meanings given below:

Controller: has the meaning given to that term in Data Protection Laws;

Data Protection Laws: means, as applicable to either party or the Services:

(a) the EU GDPR;

(b) the UK GDPR and the UK DPA 2018;

(c) any laws which implement or supplement any such laws; and

(d) any laws that replace, extend, re-enact, consolidate or amend any of the foregoing;

Data Protection Losses: means all liabilities arising directly or indirectly from any breach or alleged breach of any of the Data Protection Laws or of this Agreement, including all:

(a) costs (including legal costs), claims, demands, actions, settlements, interest, charges, procedures, expenses, losses and damages (including relating to material or non-material damage);

(b) administrative fines, penalties, sanctions, liabilities or other remedies imposed by a Supervisory Authority;

(c) compensation which is ordered by a court or Supervisory Authority to be paid to a Data Subject; and/or

(d) costs of compliance with investigations by a Supervisory Authority;

Data Subject: has the meaning given to that term in Data Protection Laws;

Data Subject Request: means a request made by a Data Subject to exercise any rights of Data Subjects under Chapter III of the GDPR in relation to any Protected Data;

EEA Data Protection Laws: means Data Protection Laws applicable under the laws of the European Economic Area, the European Union or any of their member states;

EEA Protected Data: means Protected Data to which any EEA Data Protection Laws apply;

EU GDPR: means the General Data Protection Regulation, Regulation (EU) 2016/679);

GDPR: means the EU GDPR and the UK GDPR (as applicable in the circumstances);

Joint processors: means two or more entities acting together as Processors, under the instruction of the same Controller, to process personal data on behalf of and in accordance with the instructions of that Controller under Data Protection Laws.

International Recipient: means the organisations, bodies, persons and other recipients to which Transfers of the Protected Data are prohibited under paragraph 7.1 without the Customer's prior written authorisation;

Lawful Safeguards: means such legally enforceable mechanism(s) for Transfers of Personal Data as may be permitted under Data Protection Laws from time to time;

List of Sub-Processors: means the latest version of the list of Sub-Processors used by the Supplieris available in the Annex IV of this Agreement;

Personal Data: has the meaning given to that term in Data Protection Laws;

Personal Data Breach: means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, any Protected Data;

processing: has the meaning given to that term in Data Protection Laws (and related terms such as process, processes and processed have corresponding meanings);

Processing Instructions: has the meaning given to that term in paragraph 3.1.1;

Processor: has the meaning given to that term in Data Protection Laws;

Protected Data: means Personal Data in the Customer Data;

Relevant Law: means:

(a) in respect of EEA Protected Data, all applicable law(s) of the European Economic Area and European Union and of the relevant member state(s) of either; and

(b) in respect of UK Protected Data, all applicable law(s) of the United Kingdom (or of any part of the United Kingdom);

Sub-Processor: means a Processor engaged by the Supplier or by any other Sub-Processor for carrying out processing activities in respect of the Protected Data on behalf of the Controller;

Supervisory Authority: means any local, national or multinational agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board or other body responsible for administering Data Protection Laws;

Transfer: bears the same meaning as the word 'transfer' in Article 44 of the GDPR (and related terms such as **Transfers**, **Transferred** and **Transferring** have corresponding meanings);

UK Data Protection Laws: means the Data Protection Laws applicable under the laws of the United Kingdom (or of any part of the United Kingdom), including the UK GDPR and UK DPA 2018;

UK DPA 2018: means the United Kingdom's Data Protection Act 2018;

UK GDPR: has the meaning given to that term in the UK DPA 2018; and

UK Protected Data: means Protected Data to which any UK Data Protection Laws apply.

2. JOINT PROCESSORS AND CONTROLLER

2.1 The parties agree that, for the Protected Data, the Customer shall be the Controller and the Suppliers shall be the Joint Processors. [Nothing in our Agreement relieves the Customer of any responsibilities or liabilities under any Data Protection Laws.]

2.2 To the extent the Customer is not sole Controller of any Protected Data it warrants that it has full authority and authorisation of all relevant Controllers to instruct the Suppliers to process the Protected Data in accordance with our Agreement.

2.3 The Suppliers shall process Protected Data in compliance with:

2.3.1 the obligations of Joint Processors under Data Protection Laws in respect of the performance of its obligations under our Agreement; and

2.3.2 the terms of our Agreement.

2.4 The Customer shall ensure that it, its Affiliates and each Authorised User shall at all times comply with:

2.4.1 all Data Protection Laws in connection with the processing of Protected Data, the use of the Services (and each part) and the exercise and performance of its respective rights and obligations under our Agreement, including maintaining all relevant regulatory registrations and notifications as required under Data Protection Laws; and

2.4.2 the terms of our Agreement.

2.5 The Customer warrants, represents and undertakes, that at all times:

2.5.1 the processing of all Protected Data (if processed in accordance with our Agreement) shall comply in all respects with all Data Protection Laws, including in terms of its collection, use and storage;

2.5.2 fair processing and all other appropriate notices have been provided to the Data Subjects of the Protected Data (and all necessary consents from such Data Subjects obtained and at all times maintained) to the extent required by all Data Protection Laws in connection with all processing activities in respect of the Protected Data that may be undertaken by the Suppliers and their Sub-Processors in accordance with our Agreement;

2.5.3 the Protected Data is accurate and up to date;

2.5.4 [except to the extent resulting from Transfers to International Recipients made by the Suppliers or any Sub-Processor, the Protected Data is not subject to the laws of any jurisdiction outside of the United Kingdom and European Economic Area;]

2.5.5 it shall establish and maintain adequate security measures to safeguard the Protected Data in its possession or control (including from unauthorised or unlawful destruction, corruption, processing or disclosure) and maintain complete and accurate backups of all Protected Data provided to the Suppliers (or anyone acting on their behalf) so as to be able to immediately recover and reconstitute such Protected Data in the event of loss, damage or corruption of such Protected Data by the Suppliers or any other person;

2.5.6 all instructions given by it to the Suppliers in respect of Personal Data shall at all times be in accordance with Data Protection Laws; and

2.5.7 it has undertaken due diligence in relation to the Suppliers' processing operations and commitments and it is satisfied (and at all times it continues to use the Services remains satisfied) that:

2.5.7.1 the Suppliers' processing operations are suitable for the purposes for which the Customer proposes to use the Services and engage the Suppliers to process the Protected Data;

2.5.7.2 the technical and organisational measures set out in the Annex III of our Agreement shall ensure a level of security appropriate to the risk in regards to the Protected Data as required by Data Protection Laws; and

2.5.7.3 the Suppliers have sufficient expertise, reliability and resources to implement technical and organisational measures that meet the requirements of Data Protection Laws.

3. INSTRUCTIONS AND DETAILS OF PROCESSING

3.1 Insofar as the Suppliers process Protected Data on behalf of the Customer, the Suppliers:

3.1.1 unless required to do otherwise by Relevant Law, shall (and shall take steps to ensure each person acting under its authority shall) process the Protected Data only on and in accordance with the Customer's documented instructions as set out in our Agreement (including with regard to Transfers of Protected Data to any International Recipient), as Updated from time to time (Processing Instructions);

3.1.2 if Relevant Law requires it to process Protected Data other than in accordance with the Processing Instructions, shall notify the Customer of any such requirement before processing the Protected Data (unless Relevant Law prohibits such information on important grounds of public interest); and

3.1.3 shall promptly inform the Customer if the Suppliers become aware of a Processing Instruction that, in the Suppliers' opinion, infringes Data Protection Laws, provided that:

3.1.3.1 this shall be without prejudice to paragraphs 2.4 and 2.5; and

3.1.3.2 to the maximum extent permitted by applicable law, the Suppliers shall have no liability howsoever arising (whether in contract, tort (including negligence) or otherwise) for any losses, costs, expenses or liabilities (including any Data Protection Losses) arising from or in connection with any processing in accordance with the Processing Instructions following the Customer's receipt of the information required by this paragraph 3.1.3.

3.2 [The Customer agrees that:

3.2.1 the Suppliers (and each Sub-Processor) are not obliged to undertake any processing of Protected Data that the Suppliers [reasonably] believe infringes any of the Data Protection Laws and shall not be liable (or subject to any reduction or set-off of any Fees otherwise payable to the Suppliers) to the extent that they(or any Sub-Processor) are delayed in or fail to perform any obligation under our Agreement as a result of not undertaking any processing in such circumstances; and

3.2.2 without prejudice to any other right or remedy of the Suppliers, in the event the Customer has not resolved any Processing Instruction notified to it under paragraph 3.1.3 such that it is lawful in the Suppliers' [reasonable] opinion within [30 DAYS] of such notification then SUCH FAILURE CONSTITUTES A MATERIAL BREACH OF OUR AGREEMENT BY THE CUSTOMER THAT CANNOT BE REMEDIED AND THE SUPPLIERS MAY TERMINATE OUR AGREEMENT IN ACCORDANCE WITH ITS TERMS'].]

3.3 The Customer shall be responsible for ensuring all Authorised Affiliates and Authorised Users read and understand the Privacy Policy (as Updated from time to time).

3.4 The Customer acknowledges and agrees that the execution of any computer command to process (including deletion of) any Protected Data made in the use of any of the Subscribed Services by an Authorised User will be a Processing Instruction (other than to the extent such command is not fulfilled due to technical, operational or other reasons). The Customer shall ensure that Authorised Users do not execute any such command unless authorised by the Customer (and by all other relevant Controller(s)) and acknowledges and accepts that if any Protected Data is deleted pursuant to any such command the Supplier is under no obligation to seek to restore it for free.

3.5 Subject to applicable Subscribed Service Specific Terms or the Order Form the processing of the Protected Data by the Supplier under our Agreement shall be for the subject-matter, duration, nature and purposes and involve the types of Personal Data and categories of Data Subjects set out in the Annex I of this Agreement.

4. TECHNICAL AND ORGANISATIONAL MEASURES

4.1 The Supplier shall implement and maintain technical and organisational measures:

4.1.1 in relation to the processing of Protected Data by the Supplier, as set out in theAnnex III of this Agreement; and

4.1.2 to assist the Customer insofar as is possible (taking into account the nature of the processing) in the fulfilment of the Customer's obligations to respond to Data Subject Requests relating to Protected Data, in each case at the Customer's cost on a time and materials basis in accordance with the Supplier's Standard Pricing Terms. The parties have agreed that (taking into account the nature of the processing) the Suppliers' compliance with paragraph 6.1 shall constitute the Suppliers' sole obligations under this paragraph 4.1.2.

4.2 [During the period in which the Suppliers process any Protected Data, the Customer shall regularly undertake a documented assessment of whether the security measures implemented in accordance with paragraph 4.1 are sufficient to protect the Protected Data against accidental, unauthorised or unlawful destruction, loss, alteration, disclosure or access to the extent required by Data Protection Laws in the circumstances. The Customer shall promptly notify the Suppliers of full details of any additional measures the Customer believes are required as a result of the assessment. The Customer acknowledges that the Suppliers provide a commoditised one-to-many service and the needs or assessments of other customers may differ. The Suppliers shall not be obliged to implement any further or alternative security measures, but this is without prejudice to the Customer's right to terminate our Agreement for convenience in accordance with the express provisions of our Agreement if it concludes the measures adopted by the Suppliers are no longer sufficient for its needs.]

5. USING STAFF AND OTHER PROCESSORS

5.1 Subject to paragraph 5.2, the Suppliers shall not engage (nor permit any other Sub-Processor to engage) any Sub-Processor for carrying out any processing activities in respect of the Protected Data in connection with our Agreement without the Customer's prior written authorisation. The Customer shall not unreasonably object to any new Sub-Processor (or any change to any of the Sub-Processors).

5.2 The Customer:

5.2.1 authorises the appointment of each of the Sub-Processors identified in the Annex IV of this Agreement; and

5.2.2 authorises the appointment of each Sub-Processor (or any change to any of the Sub-Processors) identified in the Annex IV as Updated from time to time. The Customer's right to object to the appointment of a new Sub-Processor (or any change to any of the Sub-Processors) following the relevant Update Notice introducing that change may be exclusively exercised by terminating our Agreement in accordance its rights following the Update Notification introducing the change before that Update takes effect in accordance with our Agreement.

5.3 The Suppliers shall:

5.3.1 prior to the relevant Sub-Processor carrying out any processing activities in respect of the Protected Data, ensure (subject to clause 8.4) that each Sub-Processor is appointed under a written contract containing materially identical obligations as under paragraphs 2 to 12 (inclusive) (including those obligations relating to sufficient guarantees to implement appropriate technical and organisational measures);

5.3.2 ensure each new Sub-Processor identified on the List of Sub-Processors further to paragraph 5.2.2 meets the following criteria at the time the addition of that Sub-Processor is first made: the Sub-Processor must possess a valid ISO 27001 certification or Cyber Essentials Plus certification at the time of their addition and meet the required standards for data protection and security under data Protection Laws.; and

5.3.3 remain fully liable for all the acts and omissions of each Sub-Processor as if they were its own.

5.4 The Suppliers shall ensure that all[natural] persons authorised by it (or by any Sub-Processor) to process Protected Data are subject to a binding written contractual obligation to keep the Protected Data confidential in a manner consistent with the Suppliers' confidentiality obligations under our Agreement.

6. ASSISTANCE WITH COMPLIANCE AND DATA SUBJECT RIGHTS

6.1 The Suppliers shall refer all Data Subject Requests it receives to the Customer without undue delay. The Customer shall pay either Supplier for all work, time, costs and expenses incurred by the Supplier or any Sub-Processor(s) in connection with such activity, calculated [on a time and materials basis] at the Suppliers' rates according to the Supplier's Standard Pricing Terms.

6.2 The Suppliers shall provide such assistance as the Customer reasonably requires (taking into account the nature of processing and the information available to the Supplier) to the Customer in ensuring compliance with the Customer's obligations under Data Protection Laws with respect to:

6.2.1 security of processing;

6.2.2 data protection impact assessments (as such term is defined in Data Protection Laws);

6.2.3 prior consultation with a Supervisory Authority regarding high risk processing; and

6.2.4 notifications to the Supervisory Authority and/or communications to Data Subjects by the Customer in response to any Personal Data Breach,

provided the Customer shall pay either Supplier for all work, time, costs and expenses incurred the Supplier or any Sub-Processor(s) in connection with providing the assistance in this paragraph 6.2 [and/or paragraph 7], calculated[on a time and materials basis] at the Supplier's rates according to the Supplier's Standard Pricing Terms.

7. INTERNATIONAL DATA TRANSFERS

7.1 Subject to paragraphs 7.2 and 7.5, the Suppliers shall not Transfer any Protected Data:

7.1.1 in or to any country or territory; and/or

7.1.2 to an organisation and/or its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries,

without the Customer's prior written authorisation except where required by Relevant Law (in which case the provisions of paragraph 3.1 shall apply).

7.2 The Customer hereby authorises the Suppliers (or any Sub-Processor) to Transfer any Protected Data for [THE PURPOSES FOR WHICH SUCH DATA MAY BE PROCESSED UNDER OUR AGREEMENT] to any International Recipient(s) in accordance with paragraph 7.3, provided all such Transfers of Protected Data to an International Recipient shall (to the extent required under Data Protection Laws) be effected by way of Lawful Safeguards and in accordance with Data Protection Laws and our Agreement. The provisions of our Agreement (including this Data Protection Agreement) shall constitute the Customer's instructions with respect to Transfers in accordance with paragraph 3.1.1.

7.3 The Suppliers (and its Sub-Processors) may only Transfer the Protected Data to (or process Protected Data in) the following countries [and territories]: UNITED KINGDOM, THE EUROPEAN ECONOMIC AREA.

7.4 The Lawful Safeguards employed in connection with Transfers pursuant to paragraph 7.2 shall be as follows: [Standard Contract Clauses].

7.5 The Customer acknowledges that due to the nature of cloud services, the Protected Data may be Transferred to recipients or other geographical locations in connection with use of the Services further to access and/or computerised instructions initiated by Authorised Users. The Customer acknowledges that the Suppliers does not control such processing and the Customer shall ensure that Authorised Users (and all others acting on its behalf) only initiate the Transfer of Protected Data to recipients or other geographical locations if Lawful Safeguards are in place and that such Transfer is in compliance with all Relevant Laws.

7.6 [The Suppliers and each Sub-Processor are not obliged to undertake any unlawful Transfer of Protected Data and shall not be liable to the extent that it (or any Sub-Processor) is delayed in or fails to perform any obligation under our Agreement due to it (or any Sub-Processor) being unable (or believing it is unable) to undertake any Transfer in a lawful manner. The Fees payable to the Supplier shall not be discounted or set-off as a result of any delay or non-performance of any obligation in accordance with this paragraph 7.6.]

8. INFORMATION AND AUDIT

8.1 The Suppliers shall maintain, in accordance with Data Protection Laws binding on the Supplier, written records of all categories of processing activities carried out on behalf of the Customer.

8.2 On request, the Suppliers shall provide the Customer (or auditors mandated by the Customer) with a copy of the third party certifications and audits to the extent made generally available to its customers[EG: ISO 27001, Cyber Essentials] (as Updated from time to time)]. Such

information shall be confidential to the Suppliers and shall be Supplier's Confidential Information as defined in our Agreement, and shall be treated in accordance with applicable terms.

8.3 [In the event that the Customer, acting reasonably, deems the information provided in accordance with paragraph 8.2 insufficient to satisfy its obligations under Data Protection Laws, the Suppliers shall, on request by the Customer make available to the Customer such information as is reasonably necessary to demonstrate the Suppliers' compliance with their obligations under this Agreementand Article 28 of the GDPR, and allow for and contribute to audits, including inspections, by the Customer (or another auditor mandated by the Customer) for this purpose provided:

8.3.1 such audit, inspection or information request is reasonable, limited to information in the Supplier's possession or control and is subject to the Customer giving the Supplier reasonable (and in any event at least 60 days') prior notice of such audit, inspection or information request;

8.3.2 the parties (each acting reasonably and consent not to be unreasonably withheld or delayed) shall agree the timing, scope and duration of the audit, inspection or information release together with any specific policies or other steps with which the Customer or third party auditor shall comply (including to protect the security and confidentiality of other customers, to ensure the Suppliers are not placed in breach of any other arrangement with any other customer and so as to comply with the remainder of this paragraph 8.3);

8.3.3 the Customer shall ensure that any such audit or inspection is undertaken during normal business hours, with minimal disruption to the businesses of the Suppliers;

8.3.4 the duration of any audit or inspection shall be limited to [ONE BUSINESS DAY];

8.3.5 all costs of such audit or inspection or responding to such information request shall be borne by the Customer, and the Suppliers' costs, expenses, work and time incurred in connection with such audit or inspection shall be reimbursed by the Customer on a time and materials basis in accordance with the Supplier's Standard Pricing Terms;

8.3.6 the Customer's rights under this paragraph 8.3 may only be exercised once in any consecutive [12] month period, unless otherwise required by a Supervisory Authority[or if the Customer (acting reasonably) believes eitherSupplier is in breach of thisAgreement];

8.3.7 the Customer shall promptly (and in any event within [ONE] Business Day) report any non-compliance identified by the audit, inspection or release of information to the Supplier;

8.3.8 the Customer agrees that all information obtained or generated by the Customer or its auditor(s) in connection with such information requests, inspections and audits shall be Suppliers' Confidential Information as defined in our Agreement, and shall be treated in accordance with applicable terms;

8.3.9 the Customer shall ensure that each person acting on its behalf in connection with such audit or inspection (including the personnel of any third party auditor) shall not by any act or omission cause or contribute to any damage, destruction, loss or corruption of or to any systems, equipment or data in the control or possession of the Suppliers while conducting any such audit or inspection; and

8.3.10 this paragraph 8.3 is subject to paragraph 8.4.]

8.4 The Customer acknowledges and accepts that relevant contractual terms agreed with Sub-Processor(s) may mean that the Suppliers or Customer may not be able to undertake or facilitate an information request or audit or inspection of any or all Sub-Processors pursuant to paragraph 8.3 and:

8.4.1 the Customer's rights under paragraph 8.3 shall not apply to the extent inconsistent with relevant contractual terms agreed with Sub-Processor(s);

8.4.2 to the extent any information request, audit or inspection of any Sub-Processor are permitted in accordance with this paragraph 8.4, equivalent restrictions and obligations on the Customer to those in paragraphs 8.3.1 to 8.3.10 (inclusive) shall apply together with any additional or more extensive restrictions and obligations applicable in the circumstances; and

8.4.3 paragraphs 5.3.1 and 8.3 shall be construed accordingly.

8.5 [Notwithstanding paragraph 8.4, the Suppliers shall ensure that it has appropriate mechanisms in place to ensure its Sub-Processors meet their obligations under Data Protection Laws [and the Suppliers' obligations in respect of Protected Data under our Agreement]. The Customer accepts that the provisions of paragraph 8.4 shall satisfy the Suppliers' obligations in that regard.]

9. BREACH NOTIFICATION

9.1 In respect of any Personal Data Breach, the Suppliers shall, without undue delay (and in any event within 72 hours):

9.1.1 notify the Customer of the Personal Data Breach; and

9.1.2 provide the Customer with details of the Personal Data Breach.

10. DELETION OF PROTECTED DATA AND COPIES

Following the end of the provision of the Services (or any part) relating to the processing of Protected Data the Suppliers shall dispose of Protected Data in accordance with its obligations under our Agreement and Annex III of this Agreement. The Suppliers shall have no liability (howsoever arising, including in negligence) for any deletion or destruction of any such Protected Data undertaken in accordance with our Agreement.

11. COMPENSATION AND CLAIMS

11.1 The Suppliers shall be liable for Data Protection Losses (howsoever arising, whether in contract, tort (including negligence) or otherwise) under or in connection with our Agreement:

11.1.1 only to the extent caused by the processing of Protected Data under our Agreement and directly resulting from the Suppliers' breach of our Agreement; and

11.1.2 in no circumstances to the extent that any Data Protection Losses (or the circumstances giving rise to them) are contributed to or caused by any breach of our Agreement by the Customer (including in accordance with paragraph 3.1.3.1 and 3.1.3.2).

11.2 If a party receives a compensation claim from a person relating to processing of Protected Data in connection with our Agreement or the Services, it shall promptly provide the other party with notice and full details of such claim.

11.3 The parties agree that the Customer shall not be entitled to claim back from either Supplier any part of any compensation paid by the Customer to the extent that the Customer is liable to indemnify or otherwise compensate the Supplier in accordance with our Agreement.

11.4 This paragraph 11 is intended to apply to the allocation of liability for Data Protection Losses as between the parties, including with respect to compensation to Data Subjects, notwithstanding any provisions under Data Protection Laws to the contrary, except:

11.4.1 to the extent not permitted by Relevant Law (including Data Protection Laws); and

11.4.2 that it does not affect the liability of either party to any Data Subject.

12. **SURVIVAL**

This Data Protection Agreementshall survive termination (for any reason) or expiry of our Agreement and continue until no Protected Data remains in the possession or control of the Supplier or any Sub-Processor, except that paragraphs 10 to 12 (inclusive) shall continue indefinitely.

Vienna, date _____ **London, date _____**

For PlanRadar GmbH and PlanRadar Limited

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 Limited
   6th Floor 2 London Wall Place
   EC2Y 5AU London
   United Kingdom

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

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

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.

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.

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.

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.

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.

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.

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.

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.

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).

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/ UK Cyber Essentials 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/UK Cyber Essentials 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 London. The storage of all data takes place within the United Kingdom.