STANDARD CONTRACTUAL CLAUSES (SCCs)
CONTROLLER TO PROCESSOR

This Standard Contractual Clauses ("SCCs") Agreement is entered into between:

1. **PlanRadar Information Technology (Sole Proprietorship L.L.C.)**
   5000 King's Fahad Road
   Riyadh
   Kingdom of Saudi Arabia

2. **PlanRadar GmbH**
   Schottenring 16, DG 1
   1010 Vienna
   Austria

subsequently called "Personal Data Importers" or "Joint Processors", or each individually referred to as a "Personal Data Importer"

INSERT Company name
INSERT Company address
Kingdom of Saudi Arabia

subsequently called „Personal Data Exporter" or "Controller", and all collectively referred to as the "Parties" agreed to the following:

1. Definitions

The Kingdom: the Kingdom of Saudi Arabia (KSA).

The Law: the Personal Data Protection Law (PDPL) issued by Royal Decree No. (M/19) dated 9/2/1443 AH and amended by Royal Decree No. (M/148) dated 5/9/1444 AH.

Regulations: the Implementing Regulations of the Law includes both implementing Regulations and the implementing Regulation for Personal Data Transfer outside the Kingdom.

The Competent Authority: Saudi Data & AI Authority (SDAIA).

Appropriate Safeguards: the requirements imposed by the competent authority on controllers, which include adherence to the Law and Regulations when transferring or disclosing personal data to entities outside the Kingdom. This applies in cases where exemptions are granted from the conditions for providing an appropriate or minimum level of personal data protection, to ensure appropriate level of protection when transferring personal data outside the Kingdom that meets at least the standards prescribed by the Law and Regulations.

International Organization: a legal body comprising members from at least three countries, operating in multiple sovereign states, established through a formal legal document such as a treaty or agreement based on international law, and this legal document defines the aims and objectives of the international organization and its structures, decision-making powers and jurisdiction. (e.g. the United Nations, the World Bank, the League of Arab States, the Arab Monetary Fund). These organizations engage in international activities and must comply with various Personal Data protection laws across different jurisdictions.

Transfer of Personal Data: transfer, disclosure (or granting of access) of Personal Data from the Kingdom of Saudi Arabia to Controllers, Processors, or other recipients in countries or international organizations other than the Kingdom of Saudi Arabia where neither the Personal Data Exporter nor the Importer of the Personal Data.

Third-Party Data Transfers/Subsequent Transfers: the transfer of Personal Data from an external country or international organization to Controllers or Processors within the same country/organization or in another country/organization.

2. Processing Instructions

2.1 The Personal Data Importer shall only process the transferred Personal Data based on written instructions from the Personal Data Exporter.

2.2 If the Personal Data Importer is unable to follow the instructions, it shall inform the Personal Data Exporter in writing without undue delay.

3. Processing Restrictions

3.1 The Personal Data Importer shall process the transferred Personal Data in accordance with the purposes specified in Annex II, unless otherwise directed in writing by the Personal Data Exporter.

3.2 Processing shall comply with the provisions of the Law and its Implementing Regulations in all cases.

4. Compliance with the Requests of the Competent Authority

4.1 In order for the Competent Authority to exercise its powers under the Law and the Implementing Regulations, the parties shall provide a copy of these Clauses to the Competent Authority upon request and without undue delay. The Competent Authority may request any additional information in relation to transfers of Personal Data.

4.2 Each party agrees to comply with any requests made by the Competent Authority in relation to these Clauses or the processing of the Transferred Personal Data.

4.3 Upon request, the Personal Data Importer (either directly or through the Personal Data Exporter) shall disclose its identity and contact details and the categories of Personal Data being processed to the Personal Data Subject and provide a copy of these items.

5. Accuracy and Quality of Personal Data

5.1 If the Personal Data Importer realizes that any Personal Data transferred is inaccurate or not up-to-date, it shall inform the Personal Data Exporter in writing without undue delay, in which case the Personal Data Importer shall destroy the Personal Data and notify the Personal Data Exporter accordingly, unless the Personal Data Exporter is instructed not to destroy the data because it wishes to correct the transferred Personal Data.

6. Duration of Personal Data Processing and Destruction or Recovery

6.1 The processing shall be carried out by the Personal Data Importer only for the period specified in Annex II. After completion of the purpose of the processing, the Personal Data Importer shall destroy all Personal Data processed on behalf of the Personal Data Exporter and notify the Personal Data Exporter accordingly unless otherwise instructed by the Personal Data Exporter in the following cases:

a) Return all processed Personal Data to the Personal Data Exporter and delete the copies held by the Data Importer;

b) If the applicable regulations in the Kingdom require the retention of the transferred Personal Data for an additional period of time;

6.2 The Personal Data Importer remains bound by these Clauses until the Personal Data is deleted or recovered.

7. Personal Data Security and Personal Data Breach Notifications

7.1 The Parties shall ensure that the organizational, administrative, and technical measures specified in Annex III provide a sufficient level of protection for the transferred Personal Data to comply with the requirements of Article (19) of the Law and Article (23) of the Implementing Regulation.

7.2 The Personal Data Importer shall implement the security measures specified in Annex III and apply those measures to all transferred Personal Data to ensure the security and protection of Personal Data against any violation that may result in damage to the Personal Data Subject, unlawful action, loss, alteration, disclosure, or unauthorized access to Personal Data.

7.3 The Personal Data Importer must periodically review the security measures stipulated in Appendix (3) to ensure that they are implemented as required and update them as needed to ensure compliance with Article (19) of the Law and Article (23) of the Implementing Regulation.

7.4 If the Personal Data Importer becomes aware of a Personal Data Breach incident that affects the transferred Personal Data or is likely to cause damage to the rights and interests of Personal Data Subjects, the Personal Data Importer must immediately take appropriate and necessary measures to contain the incident to minimize any risks or negative consequences and ensure that it is prevented from reoccurring. The Personal Data Exporter must be notified within (24) hours from the time of occurrence or knowledge of the breach incident, provided that the notification includes a description of the incident, its causes, the measures taken or planned to be taken to contain the incident and prevent its reoccurrence, in addition to the contact details for follow-up by the Personal Data Exporter. If the Personal Data Exporter realizes that the incident may cause damage to Personal Data or Personal Data Subjects or contradict their rights or interests, it shall notify the Competent Authority within (48) hours and in accordance with the requirements set out in Article (24) of the Law's Implementing Regulation.

7.5 As soon as the Personal Data Exporter receives the Data Importer's notification of a Personal Data breach incident and the incident would harm the Personal Data or the Personal Data Subject or contradict his/her rights or interests, the Personal Data Exporter must provide immediate notification in simple and clear language in accordance with the provisions of Article (24) of the Implementing Regulation to the Personal Data Subjects affected by the data breach incident, provided that the notification includes the potential risks and their nature, the measures taken or planned to be taken to contain the incident, and the contact information of the Personal Data Exporter, Data Importer, and the respective Personal Data Protection Officer of both entities, along with recommendations or consultations to aid the Data Subject in preventing or minimizing the impact of the outlined risks.

8. Sensitive Data

8.1 Without prejudice to any restrictions related to sensitive data stipulated in the Law and the Implementing Regulations of the Law, the Personal Data Exporter shall ensure that the Personal Data Importer adopts additional means of protection commensurate with the nature of the sensitive data and guarantees its protection from any risks when processing it, while ensuring that the restrictions and additional guarantees described in Annex II are applied.

9. Subsequent Transfer

9.1 The Personal Data Importer shall not transfer or disclose the transferred Personal Data to a third party outside the Kingdom unless that party has acceded to these Clauses and in accordance with the appropriate template and the provisions of Clause (7) above.

9.2 Without prejudice to the provisions of Articles (8) and (15) of the Law and (17) of the Implementing Regulation of the Law, the provisions of the Law and Regulations shall apply to Personal Data that has been previously transferred or disclosed to an entity outside the Kingdom.

10 Compliance with these Clauses

10.1 The Personal Data Importer shall respond to all inquiries of the Personal Data Exporter within the specified period and provide all information requested by the Personal Data Exporter, in addition to providing the Personal Data Exporter with all information it may request regarding the processing of the transferred Personal Data, including any information necessary to enable the Personal Data Exporter to prove its compliance with the requirements contained in these Clauses or the provisions stipulated in the Law and its Implementing Regulations.

10.2 Each party shall be responsible for demonstrating to the Competent Authority, upon request, that all obligations under these Clauses have been fulfilled.

10.3 The Personal Data Importer allows the Personal Data Exporter or its appointed representatives to audit the Data Importer's processing of Personal Data without undue delay upon Personal Data Exporter's request.

10.4 The Personal Data Exporter must provide the information revealed by the audit when requested by the Competent Authority.

10.5 The right of audit does not grant the Personal Data Exporter or its representatives access to any confidential information of the Personal Data Importer as long as this information is not closely related to the processing of the transferred Personal Data.

11 Rights of Personal Data Subjects

11.1 The Personal Data Importer shall notify the Personal Data Exporter within (48) hours from the time of receipt of the request of any request received from the Personal Data Subject, and the Personal Data Importer shall not have the right to respond to such requests unless the Personal Data Exporter authorizes it to do so.

11.2 The Personal Data Importer shall take all necessary measures in cooperation with the Personal Data Exporter to respond to the requests of Personal Data Subjects and enable them to exercise their rights under the provisions of the Law and Regulations.

11.3 The Personal Data Importer is obligated to follow all instructions issued by the Personal Data Exporter regarding the processing of the transferred Personal Data.

11.4 All statements made to the Personal Data Subject must be presented in a clear, legible, and accessible format.

Place, date _____	**Place, date _____**
For PlanRadar Information Technology and PlanRadar GmbH	**For Controller**

ANNEX I LIST OF PARTIES

Information of Personal Data Importer (s)		Information of Personal Data Exporter (s)
PlanRadar GmbH	**PlanRadar Information Technology (Sole Proprietorship L.L.C.)**	Company Name
Kärtner Ring 5-7/ Top 201 1010 Vienna Austria	**5000 King's Fahad Road Riyadh Kingdom of Saudi Arabia**	Company Address
Data Protection Officer: Constantin Köck, c.koeck@planradar.com		Contact Information
Signature		Signature
Date		Date
Role [Joint Processors]		Role [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 subprocessor, Amazon Web Services, as the cloud hosting provider.

ANNEX IV: LIST OF SUB-PROCESSORS

The Controller has authorised the use of the following sub-processor:

Oracle Systems Limited, Saudi Arabia Branch Office
Oleya, King Fahd Road,
Al Faisaliah Tower,
P.O. Box 295675,
Riyadh, Saudi Arabia

Description of the processing:

This sub-processor is used to store the data in the cloud (cloud hosting). The server location is in the Kingdom of Saudi Arabia. The storage of all data takes place within the Kingdom of Saudi Arabia.