Annex 1
Mobiess DPA for Plannon

This Data Processing Addendum (hereinafter referred to as "**Addendum**") is an addendum to the "Mobiess End User License Agreement for Planon" (hereinafter referred to as "**Agreement**") between the legal entity which has ordered the access to the Tech Partner Platform Apps and Connector Software under an Order Form (hereinafter referred to as "**Controller"**) and Mobiess Ltd (hereinafter referred to as "**Processor"**). In consideration of the obligations of each party set out in this Addendum, the parties agree as follows:

1. DEFINITIONS.

Unless otherwise defined in the Agreement, all capitalized terms used in this Addendum will have the meanings given to them below:

a. "**Processor Security Standards**" means the security standards attached to this Addendum as Annex 1;
b. "**Personal Data**" means the "personal data" (as defined in the GDPR) that is uploaded by or on behalf of Customer to the Services and/or processed by Processor under the Agreement;
c. "**Data Subject**" means identified or identifiable natural person to which the Personal Data are related.
d. "**Documentation**" means the documentation of the Services accessible in Processor's online environment, as updated or amended from time to time, including without limitation the description of the Services and the user guides as available within the Services;
e. "**EEA**" means the European Economic Area;
f. "**GDPR**" means the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679 of the European Parliament) and any national implementing laws as amended or updated from time to time. For Controllers in the UK: Unless or until it is no longer directly applicable in the UK, thereafter any successor legislation to the GDPR or the Data Protection Act 2018;
g. "**Processing**" has the meaning given to it in the GDPR and "process", "processes" and "processed" will be interpreted accordingly;
h. "**Services**" means the Tech Partner Platform Apps and Connector Software and/or related services provided by or on behalf of Processor under the Agreement.
i. **"Planon"** means the legal entity Planon International B.V. a private limited liability company, duly incorporated and existing under the laws of the Netherlands, with its principal office at Wijchenseweg 8, 6537 TL Nijmegen, the Netherlands, registered with the trade register under number 09102087 or any of its affiliate(s).
j. "**Order Form**" means an ordering document specifying the Tech Partner Platform Apps and Connector Software to be provided hereunder that is entered into between Customer and Planon.

2. DATA PROCESSING.

2.1 Scope and Roles. This Addendum applies when Personal Data is processed by Processor on behalf of Controller as required for the provision of Services in accordance with the provisions of the Agreement and this Addendum. Planon provides the cloud platform (software as a service) on which the Processor provides its Services under the Agreement to the Controller. Controller acknowledges and accepts that Personal Data will be processed on the cloud platform and may otherwise be shared with Planon subject to the terms of the data processing agreement as agreed between Planon and the Controller. The relationship between Planon and Controller and any related processing of Personal Data is governed separately from the Agreement and this Addendum

2.2 Compliance with Laws. Each party will comply with all laws, rules and regulations applicable to it and binding on it in the performance of this Addendum, including all statutory requirements relating to data protection including GDPR.

2.3 Instructions for Data Processing. Processor will process Personal Data in accordance with Controller's written instructions, unless required to do otherwise by applicable law, in which case Processor shall provide prior notice to Controller unless prohibited from doing so by law. Controller herewith instructs Processor to process Personal Data as required for the provision of Services in accordance with the provisions of the Agreement and this Addendum. Processing outside the scope of this Addendum will require prior written agreement between Processor and Controller on additional instructions for processing, including agreement on any additional fees Controller will pay to Processor for carrying out such instructions, if applicable. Processor shall not process any Personal Data for its own purposes.

2.4 Access or Use. Processor will not access or use Personal Data, except as necessary to provide the Services to Controller, unless required to do otherwise by applicable law, in which case Processor shall provide prior notice to Controller unless prohibited from doing so by a legal regulation.

2.5 Subject matter and duration of the processing. The subject matter and duration of the processing of Personal Data are as described in Annex 2 of the Addendum.

2.6 Nature and purpose of the processing. The nature and purpose of the processing of Personal Data are as described in Annex 2 of the Addendum.

2.7 Description of Data Subjects, categories of data and processing operations. Data Subjects, Categories of data, Special categories of data (if appropriate) and Processing operations are as described in Annex 2 of the Addendum. The following types of sensitive personal data (including images or other information containing or revealing such sensitive data) may not be submitted to the Services:

- government issued identification numbers;
- racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, information concerning health or sex life;
- information related to an individual's physical or mental health; and information related to the provision or payment of health care;
- Other types of sensitive personal data that are classified as special categories of personal data as referred to in Article 9 and Article 10 of the GDPR.

2.8 Disclosure. Processor will not disclose Personal Data to any third party, except as necessary to comply with this Addendum, the law or a valid and binding order of a law enforcement agency (such as a subpoena, court order or order of a competent administrative authority). If a law enforcement agency or other third party sends Processor a demand for Personal Data, Processor will attempt to redirect the law enforcement agency or other third party to request that data directly from Controller. As part of this effort, Processor may provide Controller's basic contact information to the law enforcement agency or other third party. If compelled to disclose Personal Data to a third party (including e.g. a law enforcement agency), then Processor will give Controller reasonable notice of the demand to Controller unless Processor is legally prohibited from doing so.

2.9 Processor Personnel. Processor restricts its personnel from processing Personal Data without authorisation by Processor as described in the Processor Security Standards. Processor will impose appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality.

2.10 Processing locations. Processor will comply with applicable laws when transferring Personal Data outside the EEA. Any transfers of Personal Data outside the EEA taking place at the conclusion of the Agreement are described in Annex 2 of the Addendum. Processor shall inform Controller of any intended changes concerning the addition or replacement of transfers of Personal Data outside the EEA. Controller shall be entitled to object to such changes – for a compelling reason – vis-à-vis Processor in due course.

3. SECURITY RESPONSIBILITIES OF PROCESSOR.

3.1 Processor shall take all measures required pursuant to Article 32 GDPR. The technical and organisational security measures currently implemented by Processor in this respect are described in Annex 1 of the Addendum.

3.2 The technical and organisational measures include the following:
(i) Processor has implemented and will maintain measures to maintain the security of the Services as set out in the Processor Security Standards;
(ii) Processor has implemented and will maintain measures to control access rights for Controller employees and contractors in relation to the Services as set out in article 1.1 of the Processor Security Standards. Controller has implemented and will maintain measures to control access rights to Personal Data.

3.3 Processor shall maintain the record of all categories of processing activities carried out on behalf of Controller as provided by Article 30§2 of the GDPR.

4. RESPONSIBILITIES OF CONTROLLER.

4.1 Controller is responsible for reviewing the Processor Security Standards relating to data security and making an independent determination as to whether the Services meet Controller's requirements.

4.2 Controller shall be responsible for informing Data Subjects of the processing of their data under the Agreement.

5. CERTIFICATIONS. Processor and/or its affiliate(s) hold a ISO 27001 certificate or such other alternative standards as are substantially equivalent to ISO 27001 and agree to maintain an information security program that complies with the ISO 27001 standards or such other alternative standards as are substantially equivalent to ISO 27001 for the establishment, implementation, control, and improvement of the Processor Security Standards.

6. CONTROLLER AUDIT.

6.1 Processor uses external auditors to verify the adequacy of Processor Security Standards and this Addendum. This audit: (a) will be performed annually; (b) will be performed according to ISO 27001 standards or such other alternative standards that are substantially equivalent to ISO 27001; (c) will be performed by independent third party security professionals at Processor's selection and expense; and (d) will result in the generation of a confidential audit report ("**Report**"), which will be Processor's Confidential Information.

6.2 At Controller's written request, Processor will provide Controller with a Report in order to enable Controller to reasonably verify Processor's compliance with the security obligations under this Addendum.

6.3 Controller agrees to exercise its audit right by instructing Processor to execute the audit as described in this article. With respect to requests for audits other than described in the previous sentence or other requests or instructions by Controller, Processor will respond with reasonable effort and provide Controller with information on Processor standard processes and an estimate of additional fees and costs that Controller would have to pay before Processor has to grant any requests or instructions that Processor does not offer as part of its standard services. Controller shall not be obligated to pay such additional fees or costs, unless and until Controller, at its sole discretion, agrees to such payment obligations in writing. Processor shall not be obligated to meet Controller's requests or instructions until agreement on additional payments, if any, is reached, and Processor has received such payments, if any.

7. DATA BREACH NOTIFICATION.

7.1 In accordance with article 33.2 of the GDPR, Processor shall notify the Controller without undue delay after becoming aware of a personal data breach (as defined in the GDPR).

7.2 Controller agrees that:
(i) the Controller is responsible for notifying the data breach to the competent authority within 72 hours, if notification to the competent authority is necessary pursuant to article 33 paragraph 1 of the GDPR; and
(ii) Processor's obligation to report or respond to a personal data breach under this article is not and will not be construed as an acknowledgement by Processor of any fault or liability of Processor with respect to the personal data breach.

7.3 Notification(s) of personal data breach, if any, will be delivered to one or more of Controller's administrators by any means Processor selects, including via email. It is Controller's sole responsibility that Controller has provided the accurate contact information of Controller's administrators.

8. SUB-PROCESSOR.

8.1 Authorised Sub-processor. Controller agrees that Processor may use other processer(s) ("**Sub-processor**") to fulfil its contractual obligations under the Agreement. Controller hereby consents to Processor's use of the Sub-processors listed under Annex 2 hereto, and as described in this article. Processor shall inform Controller of any intended changes concerning the addition or replacement of any Sub-processor. Controller shall be entitled to object to such changes – for a compelling reason – vis-à-vis Processor in due course.

8.2 Sub-processor Obligations. Where Processor engages a Sub-processor for carrying out specific processing activities on behalf of the Controller, similar data protection obligations as set out in this Addendum shall be imposed in writing on that Sub-processor, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of this Addendum as well as generally the mandatory requirements for data processing agreements pursuant to Art. 28 GDPR. Processor will remain responsible for its compliance with the obligations of this Addendum and for any acts or omissions of a Sub-processor that cause Processor to breach any of Processor's obligations under this Addendum.

9. LIABILITY. The limitations on liability set out in the Agreement apply to all claims made pursuant to any breach of the terms of this DPA or the GDPR.

10. CONFLICT. Except as amended by this Addendum, the Agreement will remain in full force and effect. If there is a conflict between the Agreement and this Addendum on the subject matter of this Addendum, the terms of this Addendum will control.

11. ASSISTANCE OBLIGATIONS. Processor will assist Controller, at Controller's cost, in responding to any request from a Data Subject and in ensuring compliance with its obligations under the GDPR with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators, in each case to the extent relevant to the processing carried out by Processor.

12. DATA RETURN / DATA DESTRUCTION. Upon the expiration or termination of the Agreement, unless otherwise instructed by Controller, Processor makes available to Controller data received from Controller and all data obtained or generated in connection with the Services (including Personal Data), except for data which will be (continued to be) processed on the cloud platform by Planon. Processing of such data shall be subject to the terms of the data processing agreement as agreed between Planon and the Controller. After a prior agreed period, Processor will destruct the data of Controller, except for data which will be (continued to be) processed on the cloud platform by Planon, including files, databases and backups. On request of the Controller, Processor gives proof of such destruction within thirty (30) days from such destruction.

13. APPLICABLE LAW – DISPUTES. This Addendum shall be subject to the same terms and conditions as the Agreement as regards the applicable law and the resolution of disputes.

Annex 1
Processor Security Standards

This Annex describes the technical and organizational security measures and procedures that Processor shall, as a minimum, maintain to protect the security of personal data created, collected, received, or otherwise obtain. Processor will keep documentation of technical and organizational measures identified below to facilitate audits and for the conservation of evidence.

1. INFORMATION SECURITY PROGRAM. Processor will maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to (a) secure Personal Data against accidental or unlawful loss, access or disclosure, (b) identity reasonably foreseeable and internal risks to security and unauthorized access to Personal Data, and (c) minimize security risks, including through risk assessment and regular testing. Processor will designate one or more employees to coordinate and be accountable for the information security program. The information security program will include (but not limited to) the following measures:

1.1 Access control. Processor's employees, contractors and any other persons entitled to perform the Services are only able to access the Personal Data within the scope and to the extent covered by its access permission (authorization). All services are secured with a login and a password. Customer has the possibility to adjust the password policy, e.g. the minimum password length and complexity of the password.

1.2 Network security. Processor's infrastructure will be electronically accessible to Processor's employees, contractors and any other persons as necessary to provide the Services. Processor will maintain access control and policies to manage what access is allowed to the infrastructure from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. Processor will maintain corrective action and incident response plans to respond to potential security threats.

1.3 Encryption of all data. Every data the Controller enter into Processor is fully encrypted (AES 256). In case of a data breach the data is not readable for a third party.

1.4 Human resource. Processor's employees who have access to the Personal Data will be submitted to a background check prior to access, must sign a confidentiality agreement and an annual awareness program is mandatory. They are not allowed to use the personal data for purpose other than providing Services to the Controller. Processor will further instruct its staff regarding the applicable provisions on data protection.

1.5 Supplier relationship. Processor will monitor its suppliers by reviewing the audit reports made available by the suppliers. When deemed needed by Processor other methods will be used to monitor the information security compliance. In case of non-compliance, the supplier will be contacted by Processor to address the issue and find a solution.

1.6 Disaster Recovery. Processor will maintain a disaster recovery plan in a way so it will limit the chance of downtime for the Processor. The disaster recovery plan is tested regularly.

2 CONTINUED EVALUATION. Processor will conduct periodic reviews of the security of its infrastructure and adequacy of its information security program as measured against industry security standards of Processor's choice.

3 DATA BREACH NOTICE. The Processor shall notify the Controller of any violations of the protection of personal data, providing at least the following information:

- A description of the nature of the violation, the categories concerned and the approximate number of individuals and data sets affected;
- The name and contact details of a contact partner for further information;
- A description of the likely consequences of the violation;
- A description of the steps taken in order to rectify or alleviate the violation.

Annex 2
Description of Data Subjects, categories of data and processing operations / Subject matter, duration, nature and purpose of the processing of Personal Data / Sub-processors / Transfers outside the EEA

DATA SUBJECTS.

Data Subjects include Controller's employees, agents, advisors, contractors and/or customers.
If applicable, additional Data Subjects must be additionally instructed by Controller and agreed between Processor and Controller in writing.

CATEGORIES OF DATA.

The personal data relating to individuals which is uploaded onto the Services by Controller and/or processed by Processor and/or a Sub-processor under the Agreement:
- First name and surname;
- Telephone number;
- Gender;
- Email address;
- Password
- Profile picture

If applicable, additional categories must be additionally instructed by Controller and agreed between Processor and Controller in writing.

PROCESSING OPERATIONS.

Processing through or by the Services pursuant to the Agreement.

SUBJECT MATTER, DURATION, NATURE AND PURPOSE OF THE PROCESSING OF PERSONAL DATA.

The subject matter, duration, nature and purpose of the processing of Personal Data as part of the Services, but not limited to, as follows:
Subject matter: On-line access to Software provided by Processor on behalf of Controller.
Duration: For the term during which the Services are provided as agreed in the Agreement.
Nature: On-line access to Software provided by Processor on behalf of Controller.
Purpose:
- To enable Controller access on-line the Software provided by Processor on behalf of Controller;
- To conclude and carry out the contract between Processor and Controller;
- To comply with legal obligations of Processor.

SUB-PROCESSORS AUTHORISED BY CONTROLLER.

At the conclusion of the Agreement, the Processor does not engage any Sub-processors.

TRANSFERS OUTSIDE THE EEA.

At the conclusion of the Agreement, the Processor does not transfer Personal Data outside the EEA.

CONTACT DETAILS OF PROCESSOR.

The contact details for privacy related issues are:

Email:	karl.horner@mobiess.com
Phone:	+44(0)203 411 1795

CONTACT DETAILS OF CONTROLLER

The contact details for privacy related issues are:

Name DPO (if applicable):	As specified in the Order Form]
Email address:	~~As specified~~ in the Order Form]
(reporting) Data breach email address:	As specified in the Order Form]
Phone:	As specified in the Order Form]