Data Processing Agreement
according to Art 28 GDPR

Applicable as of 23.11.2023

1. Parties
1.1. Data Controller (fill in details):

Name: as indicated in the relevant account for the Tool.

Address: as indicated in the relevant account for the Tool.

henceforth the "Controller";

1.2 Data Processor: SplitMetrics Inc, a private corporation incorporated under the laws of Delaware under No. 6041339, with its place of business at 108 W. 13th Street, Suite 100, Wilmington, DE (Delaware), 19801, henceforth the "Processor".

Signature and date: This DPA is considered to be entered by and between Controller and Processor by entering into the main contract which refers to this DPA as of the effective date of the main contract.

2. Subject of the agreement

2.1. The subject of this contract is the processing of personal data within the framework of the main contract between the Controller and the Processor. The Processor provides the Controller with App Radar ASO Tool. Within the framework of this software, the Processor will have access to the data of the Controller's customers who buy/use/comment on the Controller's App in the Apple Store or Google Play Store. These data are currently only the nicknames/usernames of users who evaluate/review the app of the Controller. Using the software provided by the Processor, the Controller can directly access and answer comments from customers.

2.2. The following categories of data are processed:

- Nicknames/Usernames

2.3. The following categories of data subjects are subject to processing:

- Clients

2.4. The processing includes (in general):

- Storage
- Reading / Queries
- Disclosure by transmission, dissemination or any other form of provision
- Matching or linking
- Restriction, deletion or destruction of data

3. Duration of the agreement

3.1. The agreement is tied to the term of the main contract.

3.2. Options for termination for good cause according to the applicable law remain unaffected, in which case this shall also be deemed to be a termination of the main contract.

4. Obligations of the Processor

4.1. The Processor undertakes to process data and results exclusively within the scope of the written orders of the Controller. The conclusion of a contract for the provision of SaaS services shall be deemed a written order. If the Processor receives an official order by authorities to surrender the Controller's customers' personal data, the Processor must - if legally permissible - immediately

inform the Controller of this and refer the authority to the Controller. Similarly, processing of the data for the Processor's own purposes requires a written order.

4.2. The Processor declares in a legally binding manner that it has obligated all persons entrusted with data processing to maintain confidentiality prior to commencement of the activity and/or that these persons are subject to an appropriate legal obligation to maintain confidentiality. In particular, the obligation of confidentiality of the persons entrusted with data processing shall remain in force even after the termination of their activities and their employment with the Processor.

4.3. The Processor declares in a legally binding manner that it has taken all necessary measures to ensure the security of the processing in accordance with Art 32 GDPR (see Annex ./1).

4.4. The Processor shall take the technical and organizational measures so that the Controller can fulfill the rights of the person concerned in accordance with Chapter III of the GDPR (information, disclosure, correction and deletion, data transferability, objection, as well as automated decision making in individual cases) at any time within the legal deadlines and shall provide the Controller with all information necessary for this purpose. If a customer of the Controller takes data protection related actions directly against the Processor, and if the Processor shows that the customer mistakenly considers him to be Controller, the Processor shall immediately forward the application to the Controller and inform the customer accordingly.

4.5. The Processor shall assist the Controller in complying with the obligations set forth in Articles 32 to 36 of the GDPR (data security measures, notification of violations of personal data protection to the supervisory authority, notification of the person affected by a violation of personal data protection, data protection impact assessment, prior consultation).

4.6. The Processor is advised that it must draw up a record of processing activities in accordance with Art 30 GDPR.

4.7. With regard to the processing of the data provided by him, the Controller is granted the right to inspect and control the data processing equipment at any time, including by third parties commissioned by him. The Processor undertakes to provide the Controller with the information necessary for checking compliance with the obligations set out in this agreement.

4.8. After termination of this agreement, the Processor is obliged to hand over all processing results and documents containing data to the Controller or to destroy them on his behalf. If the Processor processes the data in a special technical format, it is obliged to hand over the data after termination of this Agreement either in this format or, at the Controller’s request, in the format in which it received the data from the Controller or in any other common format.

4.9. The Processor shall inform the Controller without delay if it believes that an instruction from the Controller violates data protection regulations of the European Union or a relevant Member State.

4.10. Otherwise, the General Terms and Conditions of the Processor shall apply mutatis mutandis.

5. Place of performance

5.1. All data processing activities are currently carried out exclusively within the EU or EEA.

5.2. If in the future data processing activities are carried out, even if only partially, outside the EU/EEA, the Processor will ensure an adequate level of data protection. This must then result from (and/or):

- an adequacy decision of the European Commission according to Art 45 GDPR
- an exception for the particular case according to Art 49 para. 1 GDPR.
- binding internal data protection provisions pursuant to Art 47 in conjunction with Art 46 para. 2 lit b GDPR
- standard data protection clauses according to Art 46 para. 2 lit c and d GDPR.
- approved rules of conduct pursuant to Art 46 para. 2 lit e in conjunction with Art 40 GDPR.

- an approved certification mechanism pursuant to Art 46 para. 2 lit f in conjunction with Art 42 GDPR
- contractual clauses approved by the data protection authority according to Art 46 Paragraph 3 lit a GDPR
- an exception for the individual case according to Art 49 para. 1 subpara. 2 GDPR.

6. Sub-processor

6.1. The Processor may make use of sub-processors.

6.2. It shall notify the Controller of the intended use of a sub-processors in good time so that the Controller can prohibit this if necessary. The Processor shall conclude the necessary agreements with the sub-processor in accordance with Art. 28 para. 4 GDPR. In doing so, it must be ensured that the sub-processor enters into the same obligations as those incumbent on the Processor under this agreement. If the sub-processor fails to comply with its data protection obligations, the Processor shall be liable to the customer for compliance with the sub-processor's obligations.

ANNEX ./1
Technical-organizational measures

The Processor shall take appropriate technical and organizational measures to ensure a level of protection commensurate with the risk in terms of the necessary confidentiality, integrity, availability and resilience of the systems and services related to the processing on a permanent basis.

The parties have jointly determined the required level of protection (Art. 32 para. 1 GDPR).

The parties have come to the conclusion that the risk of the processing is to be classified as "high" and therefore a high level of protection must be maintained.

The high level of protection is maintained by these measures:

1. Confidentiality (Art. 32 para. 1 lit. b GDPR)

Area control

No unauthorized access to data processing systems. The office is lockable with keys. Access to physical servers is only possible through biometric security systems.

Access control

No unauthorized system use. Data is only accessible through accounts with secure passwords and appropriate clearance.

Authorization control

No unauthorized reading, copying, modification or removal within the system. Authorization concepts and needs-based access rights, logging of accesses and modifications (full versioning);

Separation control

Separate processing of data collected for different purposes, e.g. multi-Controller capability, sandboxing;

Pseudonymisation (Art. 32 (1) lit. a GDPR; Art. 25 (1) GDPR)

The processing of personal data in such a way that the data can no longer be assigned to a specific data subject without the inclusion of additional information, provided that this additional information is kept separately and is subject to appropriate technical and organizational measures;

2. Integrity (Art. 32 Paragraph 1 lit. b GDPR)

Transmission control

No unauthorized reading, copying, modification or removal during electronic transmission or transport, e.g: encryption, Virtual Private Networks (VPN), electronic signature;

Input control

Determining whether and by whom personal data have been entered, modified or removed from data processing systems, e.g.: logging, document management;

3. Availability and Resilience (Art. 32 para. 1 lit. b GDPR)

Availability control

Protection against accidental or wilful destruction or loss, e.g: A5] Backup strategy (online/offline; on-site/off-site), uninterruptible power supply (UPS), virus protection, firewall, reporting channels and emergency plans;

Rapid recoverability (Art. 32 para. 1 lit. c GDPR);

4. Procedures for regular review, assessment and evaluation (Art. 32 para. 1 lit. d GDPR; Art. 25 para. 1 GDPR)

Data protection management;
Incident response management;
Data protection-friendly default settings (Art. 25 para. 2 GDPR);

Instruction control

No commissioned data processing within the meaning of Art. 28 GDPR without corresponding instructions from the Controller, e.g: Clear contract design, formalised order management, strict selection of the service provider, obligation to convince in advance, follow-up checks.