Annex 5
Confidential

ANNEX 5 – Data Processing Annex

Annex 5
Confidential

1. Background, purpose & rules in case of conflict

This Data Processing Annex (”**DPA**”) sets out the terms and conditions for the processing of Personal Data by Navigil on behalf of Customer under Agreement between the Parties. This DPA is an essential and inseparable part of Agreement.

Navigil (hereinafter ”**Supplier**”) acts as a processor and Customer acts as a controller of Personal Data, the concepts of which shall have the meaning given in Data Protection Regulation. For the sake of clarity, it is stated that Customer may also act on behalf of its customer company that de facto is a data controller of Personal Data as defined in Data Protection Regulation. In such case, Customer warrants that Customer is acting based on an authorization of such third-party data controller in relation to Personal Data processed, and that the terms of Customer’s agreement with each such third-party data controller are consistent with this DPA.

In the event of any discrepancy between the content of the body of this DPA, Agreement or any of the other Appendices to Agreement, or Data Protection Regulation, the following order of precedence shall be applied:

i. Data Protection Regulation
ii. This DPA and any Appendices to this DPA
iii. Agreement and any other Appendices to Agreement

2. Definitions

”**Data Protection Regulation**” means all applicable laws relating to protection of Personal Data in the European Union, including without limitation the GDPR and the national laws supplementing the GDPR and the laws implementing EU Directive 2002/58/EC.

”**Data Subject**” means a natural person whose Personal Data is processed by Supplier under Agreement and this DPA.

”**GDPR**” means the EU General Data Protection Regulation (2016/679/EC) and any amendments thereto.

”**Personal Data**” means any information relating to an identified or identifiable natural person, which Supplier is processing under Agreement. In this regard, processing means any operation, or set of operations, performed by Supplier on Personal Data, by any means, such as collecting, organizing, storing, amending, retrieving, using, disclosing, transmitting, combining, blocking, erasing or destructing Personal Data.

”**Personal Data Breach**” means a breach of security leading to destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed, which is adverse to Data Protection Regulation.

”**SCC**” means the standard contractual clauses issued by the European Commission by the decision 2010/87/EU for international transfers of Personal Data, and any amendments thereto.

3. Personal Data processed under this DPA

Supplier shall process Personal Data under this DPA solely for the purpose of fulfilling its obligations under Agreement. Notwithstanding the foregoing, Supplier shall have the right to use, exploit, modify, amend and reproduce anonymized Personal Data (”**Anonymized Data**”) for its business purposes, including but not limited to the development, enhancement and modification of Services (as defined in Agreement) or services similar to Services. Customer acknowledges that Anonymized Data shall not be considered as Personal Data. The rights and obligations set out in this DPA shall not be applied to Anonymized Data.

The categories of Personal Data processed under this DPA shall contain contact information, user names and location information (GPS), information relating to personal details of Data Subjects, information related to alarm calls, wellness data (e.g. heart rate, respiration rate and other health tracker data collected by the wristwatch) and other necessary Personal Data for the purposes of Supplier fulfilling its obligations under Agreement.

The categories of Data Subjects whose Personal Data is processed under this DPA shall contain End Users and other natural persons using Services.

Regardless of above, Supplier shall have the right to process Personal Data in connection with Agreement as necessary for provision, development and technical functioning of Services (as defined in Agreement), customer service and other management of customer relations, billing, communications, marketing and other corresponding purposes, which may relate to employees and contact persons of Supplier (”**Supplier's Personal Data**”). Supplier shall act as data controller of Supplier's Personal Data and remains responsible for the lawful processing thereof

4. Rights and responsibilities of customer

Customer shall process Personal Data in compliance with all applicable laws and regulations in its respective jurisdiction, including but not limited to Data Protection Regulation.

Customer's complete documented instructions on processing of Personal Data are given in this DPA. Customer shall have the right to give Supplier new documented instructions or amend the documented instructions given by Customer to Supplier. Customer's new documented instructions to Supplier require a written agreement between Parties. Supplier is entitled to charge for additional costs for complying with new or amended documented instructions from Customer.

5. Responsibilities of Supplier

5.1 General principles applicable to processing of Personal Data

Supplier shall:

a) process Personal Data in compliance with Data Protection Regulation and good data processing practice;

b) process Personal Data on documented instructions from Customer as defined in Section 4, unless prescribed otherwise by a provision of Data Protection Regulation applicable to Supplier. In such case, Supplier shall inform the Customer of such requirement in reasonable time before beginning the processing of Personal Data in accordance with the instructions, unless informing of such requirement is prohibited in Data Protection Regulation. In case Supplier considers that instructions of Customer are in breach of Data Protection Regulation, Supplier shall inform Customer without undue delay;

c) ensure that Supplier's staff with access to Personal Data have committed themselves to appropriate confidentiality;

d) carry out the measures prescribed in section 5.2 of this DPA;

e) follow the conditions concerning the use of subcontractors as prescribed in Section 8 of this DPA;

f) taking into account the information available to Supplier, provide reasonable assistance to Customer in responding to requests for exercising the rights of Data Subjects where Customer does not have the needed information. Supplier is entitled to charge Customer for costs and expenses that were incurred as a result of complying with this clause 5.1.f;

g) taking into account the information available to Supplier, provide reasonable assistance to Customer in ensuring compliance with its obligations set out in Data Protection Regulation, relating to data security, Personal Data Breaches, data protection impact assessments, and prior consulting obligations. Supplier is entitled to charge Customer for costs and expenses that were incurred as a result of complying with this clause 5.1.g;

h) at the choice of Customer, delete or return Personal Data to Customer as prescribed in Section 10 of this DPA;

i) make available to Customer all information necessary to demonstrate compliance with obligations set out in this

DPA and in Data Protection Regulation. Customer is obliged to keep all such information confidential. Supplier is entitled to charge Customer for costs and expenses that were incurred as a result of complying with this clause 5.1.i; and

j) allow Customer to perform audits as prescribed in Section 9 of this DPA.

5.2 Data security

Supplier shall implement technical and organizational measures to ensure an appropriate level of security to protect Personal Data against unauthorized access and loss, destruction, damage, alteration or disclosure, or against other unlawful processing.

6. Personal Data Breach notification

Supplier shall notify Customer of all Personal Data Breaches without undue delay after Supplier has become aware of the Personal Data Breach. The notification shall contain the following:

a) description of the nature of the Personal Data Breach, including the categories and approximate number of Data Subjects concerned and the categories and approximate number of data records concerned;

b) name and contact details of the contact person of Supplier handling the Personal Data Breach;

c) description of likely consequences and/or realized consequences of the Personal Data Breach; and

d) description of the measures Supplier has taken to address the Personal Data Breach and to mitigate its adverse effects.

If it is not possible to provide the information listed in above in a) – d) at the same time, the information may be provided in phases.

Supplier shall document Personal Data Breaches and disclose the documentation to Customer upon Customer's request.

After Supplier has become aware of Personal Data Breach, Supplier shall ensure security of Personal Data and take appropriate measures to ensure protection of Personal Data in cooperation with Customer.

7. Transfers of Personal Data

Supplier uses Amazon Web Services to provide hosting of the Services. Depending on the location of Customer, the Services are hosted either in Europe (Ireland), USA or Japan.

Supplier and its subcontractors shall process Personal Data within European Economic Area (”**EEA**”). Personal Data may be transferred outside of EEA under the following conditions:

a) Where Customer is established in EEA, Supplier shall not transfer Personal Data outside of EEA without Customer's prior approval thereto. Customer hereby consents to such transfer of Personal Data outside of EEA and authorizes Supplier to enter into a data transfer agreement with its subcontractors incorporating SCC in the name and on behalf of Customer.

b) Where Customer is established outside of EEA, Supplier shall be entitled to transfer Personal Data outside of EEA for the purpose of providing the Services to Customer. In such case, Supplier shall comply with the Data Importer's obligations as set out in the SCC.

8. Subcontractors

Supplier is entitled to use subcontractors in processing of Personal Data. Supplier shall disclose the list of subcontractors used at the time of signing Agreement to Customer upon Customer's request.

Supplier shall notify Customer about an addition of a subcontractor processing Personal Data under this DPA at least thirty (30) days before the subcontractor begins processing Personal Data. Customer may object to the use of the new subcontractor only if Customer has well-grounded doubts about the ability of the subcontractor to comply with Data Protection Regulation. If Customer does not object to the use of the new subcontractor in writing in fourteen (14) days from notice of Supplier, Supplier may use the new subcontractor in processing Personal Data. Supplier is entitled to reduce the number of subcontractors without separate notice.

Supplier shall take appropriate measures to ensure that the used subcontractors comply with the obligations specified in this DPA, including security and confidentiality requirements. Supplier is responsible for the performance of its subcontractors as it is responsible for the performance of its own obligations.

9. Auditing

Customer is entitled to audit Supplier's compliance with obligations set out in this DPA in order for Customer to ensure that Supplier has fulfilled the obligations set out in this DPA. The Parties agree that when Customer requests for an audit, a third party appointed or approved in writing by Supplier shall perform the audit. Customer has the right to request an audit prescribed in this Section 9 once in every twelve (12) months.

Each Party shall bear its own costs and expenses in connection with the audit, and Customer shall bear the fees and expenses of the third party. If the audit reveals substantive shortcomings, Supplier shall bear the costs and expenses incurred by Supplier and reasonable fees and expenses of the third party.

Supplier shall assist Customer and the third party in conducting the audit with reasonable measures.

If the audit reveals shortcomings, Supplier shall correct such shortcomings without delay or at the latest within thirty (30) days of a written notice from Customer, unless the Parties agree otherwise. Any material shortcomings that pose an obvious threat to security of Personal Data shall be rectified without delay.

10. Duration of processing Personal Data

Supplier shall process Personal Data only during the term of Agreement and after that if required by applicable law or contractual obligations or rights of either Party.

Upon termination or expiry of Agreement, or upon Customer’s written request, Supplier shall either destroy or return, either to Customer or to a third party designated by Customer in writing, Personal Data processed, unless otherwise required by Data Protection Regulation or other applicable legislation. In case Customer demands Personal Data to be returned to Customer or transferred to a third party, Customer will pay Supplier for any additional costs caused by return or transfer of Personal Data.

For the sake of clarity, the Parties acknowledge that the obligations set out above in this Section 10 shall not prevent Supplier from processing Supplier's Personal Data or Anonymized Data during or after the term of Agreement.