DATA PROCESSING AGREEMENT

This Data Processing Agreement was last updated on April 14, 2023. The records of the previous versions of the Data Processing Agreement can be found here:

Version of July 22, 2021

Version of September 17, 2021

Version of December 20, 2022

This Data Processing Agreement, including its Exhibits and Appendices ("*DPA*") forms an addendum to the Master Subscription Agreement or the Terms of Use between Aircall and Customer for the purchase of Services, including any and all applicable Order Form(s), Purchases, exhibits and/or schedules (the "*Agreement*").

In the course of providing the Services to Customer pursuant to the Agreement, Aircall may Process Personal Data on behalf of Customer. This DPA reflects the parties' agreement with regard to the Processing of Personal Data.

The Parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

DEFINITIONS

All capitalized terms not defined herein shall have the meaning ascribed to them in the Agreement. In this DPA, the following capitalized terms used shall further have the meanings given to them below:

The terms "*Data Controller*" and "*Data Processor*" shall have the meaning ascribed by the GDPR. The terms "*Data Subject*", "*Personal Data*" and "*Process, Processing*" shall have the meaning ascribed by the GDPR, but shall only cover the scope of personal data processing specified in Exhibit A of this DPA. However, in case that the Applicable Data Protection Laws define these terms differently and the GDPR does not apply to the Processing, the definition set forth by the Applicable Data Protection Laws shall apply instead of the definition ascribed by the GDPR. In case that the Applicable Data Protection Laws define these terms differently and the GDPR applies to the Processing, the definition provided in the GDPR will prevail. In case the Applicable Data Protection Laws define terms, which have the same or materially similar meaning to the terms "Data Controller", "Data Processor", "Data Subject", "Personal Data" and/or "Process, Processing", such terms will be considered as covered correspondingly by the definitions provided herein.

The terms "Business Associate Agreement", "Covered Entity" and "Protected Health Information" shall have the meaning ascribed by HIPAA and shall be interpreted in accordance with relevant regulations issued by the U.S. Department of Health and Human Services.

"Admin User Email Address" means every email address associated with the Customer's account with Aircall in the way that it is, at the given point of time, registered by Aircall as an email address of an admin user of the Customer's account.

"*Applicable Data Protection Laws*" means all data protection laws and regulations applicable to the Processing of Personal Data under this DPA, which may, depending on the

circumstances, include but not be limited to the European Data Protection Laws and/or HIPAA, as defined below.

“Data Breach” means a personal data breach concerning Personal Data, which is likely to result in a risk to the rights and freedoms of the Data Subjects.

“*EEA*” means the European Economic Area.

“EU *GDPR*” means Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

“European Data Protection Laws” means the GDPR and/or the FADP, as applicable to the Personal Data Processing in question.

“*FADP*” means the Federal Act on Data Protection adopted by the Federal Assembly of the Swiss Confederation, as amended.

“GDPR” means the EU GDPR and/or the UK GDPR, as applicable to the Personal Data Processing in question.

"HIPAA" means the United States’ Health Insurance Portability and Accountability Act of 1996.

”EU *Standard Contractual Clauses for Data Transfers to Third Countries*” means the standard contractual clauses as approved by the European Commission’s decision 2021/915 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to the EU GDPR, and any amendments thereto.

”*Subprocessor*” means any legal entity, including a subcontractor, engaged by Aircall to Process all or part of the Personal Data for Aircall on behalf of the Customer.

“UK GDPR” has the meaning given to it in section 3(10) of the UK Data Protection Act 2018.

“UK International Data Transfer Addendum” means the International Data Transfer Addendum to the EU Standard Contractual Clauses, issued by the Information Commissioner and laid before Parliament in accordance with s.119A of the UK’s Data Protection Act 2018 on 2 February 2022 and any amendments thereto.

1. APPLICATION OF DATA PROTECTION LAWS AND THE TERMS

1.1 Compliance with Applicable Data Protection Laws. The Customer hereby represents that this DPA complies, to its reasonable knowledge, with all Applicable Data Protection Laws and contains all provisions required by such laws. Considering the nature of the Services, the Customer acknowledges that the Processing of Personal Data under this DPA may be subject to various Applicable Data Protection Laws, even those which are not explicitly mentioned in this DPA, depending on the territorial extent of Customer’s usage of the Services. The Customer is responsible for informing Aircall without undue delay about any discrepancy between this DPA and the requirements of the Applicable Data Protection Laws.

1.2. Applicability of the European Data Protection Laws, roles of the Parties. The parties acknowledge that GDPR applies to the Processing of Personal Data if and to the extent conditions set forth by Art. 3 of the GDPR are fulfilled. The parties further acknowledge that the FADP applies to the Processing of Personal Data if and to the extent conditions set forth by the FADP are fulfilled. To the extent the European Data Protection

Laws apply to the Processing of Personal Data under this DPA, the Customer may act as a Data Controller and/or a Data Processor and Aircall acts as a Data Processor. Where the Customer acts as a Data Processor and engages Aircall as another Data Processor in accordance with Art. 28(4) of the GDPR, the Customer:

a) Is responsible for ensuring that the same data protection obligations as set out in the contract or other legal act between the Customer and the Data Controller of the Personal Data are hereby imposed on Aircall;

b) Is responsible for ensuring that the instructions provided by the Customer to Aircall under Section 2.4 of this DPA do not violate the contract or other legal act between the Customer and the Data Controller of the Personal Data;

c) Assumes the rights and responsibilities of Data Controller towards Aircall under this DPA, therefore whenever this DPA refers to a "Data Controller", such reference shall equally refer to the Customer, and vice versa; and

d) Remains fully liable to the Data Controller of the Personal Data where Aircall fails to fulfil its data protection obligations hereunder.

1.3. Applicability of HIPAA. The Customer understands and agrees that it must separately enter into and execute a Business Associate Agreement ("BAA") if (1) Customer qualifies as a Covered Entity or Business Associate and (2) Customer will make Protected Health Information available to Aircall in connection with performing the Agreement, to the extent such Protected Health Information is collected from patients in the United States and its territories and possessions. Where the parties have entered into a BAA, the BAA shall take precedence over this DPA with respect to any Protected Health Information collected from patients in the United States and its territories and possessions.

2. PROCESSING OF PERSONAL DATA

2.1. Customer's Processing of Personal Data. Customer determines the purposes and means of the Processing of Personal Data. Customer's instructions for the Processing of Personal Data shall comply with Applicable Data Protection Laws.

2.2. Customer's liability. The Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data provided by the Customer to Aircall and the means by which Customer acquired such Personal Data. To the extent the European Data Protection Laws apply to the Processing of Personal Data under this DPA, the Customer is liable for complying with its obligations as Data Controller, including informing the Data Subjects about the Processing of their Personal Data under this DPA, obtaining their consent, if necessary, and ensuring that the Customer and Aircall have the authority to use the Personal Data in accordance with the purposes defined herein.

2.3. Aircall's Processing of Personal Data. Aircall shall only Process Personal Data on behalf of and in accordance with Customer's documented instructions, including in relation to transfers of Personal Data. Notwithstanding the above, Customer hereby explicitly acknowledges that Aircall may process Personal data, as a separate Data Controller, for other processing purposes in compliance with the Applicable Data Protection Laws, e.g. in case of Aircall's legitimate interest on such processing or when applicable laws require such processing from Aircall. Aircall, as a Data Controller, remains responsible for the processing of Personal Data described in the previous sentence; and this DPA does not apply to such processing of the Personal Data. Aircall provides more information about its processing of Personal Data in Aircall's Privacy Policy: https://aircall.io/privacy/. Where necessary under

the Applicable Data Protection Laws, Aircall shall further restrict its Processing of Personal Data that qualifies as customer proprietary network information within the meaning of 47 U.S.C. § 222 as may be required by law and implementing regulations issued by the Federal Communications Commission.

2.4. Customer's Instructions. Customer instructs Aircall to Process Personal Data for the provision of Services, as specified in more detail in Exhibit A hereof. The Parties agree that this DPA, the Agreement, instructions provided via configuration tools incorporated in Aircall's platform and instruction provided via Aircall's dedicated customer support portal constitute Customer's complete and final instructions to Aircall for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately in writing.

2.5. Obligations of Aircall. To the extent set forth by the Applicable Data Protection Laws, Aircall agrees, warrants and represents that it:

a) Ensures that persons authorized to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; further, Aircall shall only allow access to the Personal Data to such of the Aircall's personnel who need access to the Personal Data in order to allow Aircall to perform its obligations under the Agreement;

b) Informs immediately the Customer if, to Aircall's knowledge, an instruction infringes the Applicable Data Protection Laws;

c) Takes all measures to ensure the confidentiality of Personal Data and the security of Processing, as further specified in Section 3 hereof;

d) Assists the Customer in ensuring compliance with the obligations relating to the security of the Personal Data (as further specified in Section 3 hereof), Customer's notification & communication obligations in case of Data Breach (as further specified in Section 7 hereof), conducting data protection impact assessments (or a similar assessment as designated by the Applicable Data Protection Laws) and consulting the supervisory authority if need be, taking into account the nature of Processing and the information available to Aircall; and

e) Makes available to the Customer on a reasonable basis all information necessary to demonstrate compliance with the obligations relating to Aircall as laid down in this DPA and in the Applicable Data Protection Laws, if applicable.

3. SECURITY OF PERSONAL DATA

3.1. Technical and Organizational Measures. Aircall shall, while taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of Processing as well as the risks of varying likelihood and severity for rights and freedoms of Data Subjects resulting from the Processing, implement appropriate technical and organizational measures listed in Exhibit B.

3.2. Reviews and Updates. The technical and organizational measures shall be reviewed and updated by Aircall where and when necessary. The Customer agrees that Aircall may unilaterally update the technical and organizational measures from time to time provided that such updates do not result in a material reduction of the level of protection of the Personal Data. Aircall's obligation under Section 3.1 hereof remains unaffected.

3.3. Information. Aircall will provide the Customer with more information about securing, accessing and using Personal Data, anytime upon Customer's request.

4. RIGHTS OF DATA SUBJECTS AND OTHER REGULATORY ACTIONS

4.1. Data subjects' right to information. It is the Customer's responsibility to provide the Data Subjects with the information on the processing of their Personal Data.

4.2. Exercise of data subjects' rights. To the extent set forth by the Applicable Data Protection Laws, Aircall shall assist the Customer, insofar as this is possible, for the fulfilment of its obligation to respond to Data Subject right requests concerning notably the right of access, to rectification, erasure and to object, right to restriction of processing, right to data portability, right not to be subject to an automated individual decision (including profiling).

4.3. Regulatory Action. If Aircall receives notice (whether or not from the Customer) of, any claim, complaint, request, direction, query, investigation, proceeding or other action of any Data Subject, court, regulatory or supervisory authority, or any body, organization or association in each case which relates in any way to the Personal Data Processed by Aircall under this DPA (collectively, "*Regulatory Action*"), then Aircall shall, if and to the extent required by the Applicable Data Protection Laws:

a) Notify the Customer via email sent to the Admin User Email Address with reasonable detail of the Regulatory Action, including copies of any relevant correspondence so that the Customer can deal with the Regulatory Action;

b) Provide the Customer with reasonable cooperation and assistance by appropriate technical and organizational measures with respect to any Regulatory Action; and

c) Not answer to a Regulatory Action, unless instructed otherwise by the Customer in writing or unless Aircall is required to answer under the Applicable Data Protection Laws.

5. SUBPROCESSORS

5.1. List of Subprocessors. Customer agrees that Aircall engages Subprocessors in connection with the provision of Aircall's Services and that the list of the Subprocessors currently engaged by Aircall is listed on Aircall's website: here. Therefore, by entering to this DPA, Customer authorizes Aircall to engage the Subprocessors mentioned in this list.

5.2. General authorization. By executing the DPA, the Customer further grants Aircall with a general authorization to engage other Subprocessors, add or replace the Subprocessors in the list. In case the list of Subprocessors is modified by Aircall, Customer will be informed of any intended changes via email to the Admin User Email Address. This information will clearly indicate which processing activities are being subcontracted out, the name and contact details of the intended subprocessor.

5.3. Objections. To the extent Applicable Data Protection Laws grants Customer the right to object against intended modifications concerning the addition or replacement of the Subprocessors, the Customer may reasonably object to such modification. In case Customer does not send any objection to Aircall in writing within ten (10) days from receiving the information, it will be deemed to have agreed to the new Subprocessors. If Customer objects, the Parties agree to negotiate to find a solution that will satisfy both Parties' interests.

5.4. Same obligations. Where Aircall engages another Subprocessor, it shall do so by way of a contract which imposes on the Subprocessor the same obligations as the ones imposed on Aircall under this DPA. Aircall shall ensure that the Subprocessor complies with the obligations to which the data processor is subject pursuant to this DPA and the Applicable Data Protection Laws.

5.5. Subprocessor agreements. To the extent required by the Applicable Data Protection Laws and permitted by Aircall's confidentiality obligations, Aircall may provide, at the Customer's request, a copy of such a Subprocessor agreement and subsequent amendments to the Customer.

5.6. Liability. To the extent set forth by the Applicable Data Protection Laws, Aircall shall be liable towards the Customer for the acts and omissions of its Subprocessors to the same extent Aircall would be directly liable if performing the Services of each Subprocessor directly under the terms of this DPA.

6. INTERNATIONAL DATA TRANSFERS

6.1. Locations of Processing. Aircall hereby represents that it will Process Personal Data under this DPA exclusively in the country of Aircall's residence and in the countries designated in the list of Aircall's Subprocessors maintained under Section 5.1 hereof.

6.2 European Personal Data transfers subject to appropriate safeguards. The locations described is Section 6.1 hereinabove may include countries located outside the EEA, UK and Switzerland and, for the purposes of the applicable European Data Protection Law, (i) have not been recognized by the relevant authority as providing an adequate level of protection for personal data (as described in the applicable European Data Protection Law) or (ii) are not covered by a suitable framework recognized by the relevant authorities or courts as providing an adequate level of protection for personal data ("*Locations Subject to Appropriate Safeguards*"). Where the Processing of Personal Data is subject to the European Data Protection Law, the Parties shall not transfer Personal Data to any Location Subject to Appropriate Safeguards, unless the Parties have taken measures necessary to ensure that the transfer complies with the applicable European Data Protection Law.

6.3 EEA and Swiss Personal Data transfers to Aircall. Where the Processing of Personal Data consists of or includes a transfer of Personal Data from the Customer, whose activities are subject to the EU GDPR or the FADP, to Aircall, who is in a Location Subject to Appropriate Safeguards and whose activities are not subject to the EU GDPR or the FADP, the EU Standard Contractual Clauses for Data Transfers to Third Countries will apply and are hereby incorporated to this DPA. If necessary, Aircall shall apply supplementary measures to ensure that the Personal Data transferred hereunder receives an essentially equivalent protection as that guaranteed in its original jurisdiction. For the purposes of the EU Standard Contractual Clauses for Data Transfers to Third Countries hereunder:

a) The Customer acts as a data exporter and Aircall acts as a data importer;

b) Where the Customer acts as a Data Controller, Module 2: Transfer controller to processor will apply;

c) Where the Customer acts as a Data Processor, Module 3: Transfer processor to processor will apply;

d) Clause 7 – Optional - Docking clause, will apply;

e) In Clause 9 – Use of sub-processors, Option 2 will apply, and the period for prior notice of sub-processor changes shall be ten (10) business days;

f) In Clause 11 - Redress, the optional language will not apply;

g) In Clause 12 - Liability, any claims brought under the EU Standard Contractual Clauses for Data Transfers to Third Countries shall be subject to the terms and conditions set forth in this Agreement, whereby in no event shall any Party limit its

liability with respect to any Data Subject rights under the EU Standard Contractual Clauses for Data Transfers to Third Countries;

h) In Clause 17 – Governing law, Option 1 will apply, the clauses will be governed by the laws of France;

i) In Clause 18(b) - Choice of forum and jurisdiction, disputes shall be resolved before the courts of France;

j) Annex I(a) – List of Parties, shall be deemed completed with the following information:

    i) The names and addresses of the data exporter and the data importer: as identified in the Agreement;

    ii) The contact details of the data importer: the Admin User Email Address;

    iii) The contact details of the data exporter: privacy@aircall.io;

    iv) Activities relevant to the data transferred under these Clauses: identified in the list of Subprocessors (Section 5.1 of the DPA);

    v) Signature and date: detailed in the Agreement;

k) Annex I(b) – Description of Transfer, shall be deemed completed with the following information:

    i) Categories of data subjects whose personal data is transferred, purpose(s) of the data transfer and further processing and the period for which the personal data will be retained: detailed in Exhibit A of the DPA;

    ii) Categories of personal data transferred: detailed in Exhibit A of the DPA; if sensitive data are transferred, the following safeguards apply: sensitive data may only be contained in the Call/SMS content; strict purpose limitation (Call/SMS content is not used for any other purpose than Provision of Aircall product and services; access restrictions (including access only for staff having followed specialised training and only based on explicit consent of the Data exporter's representative); keeping a record of access to the data;

    iii) The frequency of the transfer: Personal data is transferred on a continuous basis;

    iv) Subject matter, nature and duration of the processing or transfers to subprocessors: identified in the list of Subprocessors (Section 5.1 of the DPA);

    v) Signature and date: detailed in the Agreement;

l) For the purposes of Annex I(c) – Competent Supervisory Authority, the competent supervisory authority in accordance with Clause 13 of the EU Standard Contractual Clauses for Data Transfers is the Commission nationale de l'informatique et des libertés (CNIL);

m) Annex II – Technical and Organizational Measures including Technical and Organizational Measures to Ensure the Security of the Data, shall be deemed completed with the information inserted in Exhibit B of this DPA; and

n) For the purposes of Annex III - List of Sub-processors, the data exporter has authorised the use of the Subprocessors detailed in Section 5.1 of the DPA and the list of Subprocessors referred to therein.

6.4 UK Personal Data transfers to Aircall. Where the Processing of Personal Data consists of or includes a transfer of Personal Data from the Customer, whose activities are subject to the UK GDPR, to Aircall, who is in a Location Subject to Appropriate Safeguards and whose activities are not subject to the UK GDPR, the UK International Data Transfer Addendum will apply. As permitted by clause 17 of such addendum, the Parties agree to change the format of the information set out in Part 1 of the addendum so that:

a) The details of the Parties in table 1 shall be deemed completed with the information inserted or referenced in the Agreement, including the references in Section 6.3 of this DPA;

b) For the purposes of table 2, the UK International Data Transfer Addendum shall be deemed appended to the EU Standard Contractual Clauses for Data Transfers as defined in Section 6.3 of this DPA (including the selection of modules and options and the disapplication of optional clauses as defined in Section 6.3 of this DPA);

c) The appendix information listed in table 3 shall be deemed completed with the information inserted or referenced in Section 6.3 hereof; and

d) For the purposes of table 4, either the data importer or data exporter may end this addendum as set out in clause 19 of the Addendum.

6.5 European Personal Data onward transfers. Where the Processing of Personal Data consists of or includes a transfer of Personal Data from Aircall, whose activities are subject to the European Data protection Law, acting as a data exporter, to a third party, who is in a Location Subject to Appropriate Safeguards and whose activities are not subject to the European Data protection Law, acting as a data importer (including, but not limited to, the Subprocessors), Aircall may transfer the Personal Data to the third party only if conditions of Section 6.2 hereof are met.

6.6. Conflict. In the event of any conflict or inconsistency between this DPA and the EU Standard Contract Clauses for Data Transfers to Third Countries incorporated herein, the EU Standard Contractual Clauses for Data Transfers to Third Countries shall prevail.

7. DATA BREACHES

7.1. Notification. Aircall will notify Customer of any Data Breach promptly after detection of such Data Breach by Aircall. Where a European Data Protection Law applies, Aircall will notify Customer no later than 24 hours after such detection. The notification shall be carried out via email sent to Admin User Email Address.

7.2. Provided information. Aircall undertakes to provide the Customer with all reasonable cooperation and assistance, as well as all details of the Data Breach required for the Customer to comply with its obligations under the Applicable Data Protection Laws in relation to the Data Breach.

8. AUDIT RIGHTS

8.1. Customer audit right. If and to the extent such right is granted to the Customer by the Applicable Data Protection Laws, Customer or its independent third party auditor reasonably acceptable to Aircall (which shall not include any third party auditors who are

either a competitor of Aircall or not suitably qualified or independent) may audit practices relevant to Personal Data Processing by Aircall, if:

a) The Customer has reasonable grounds, proved in advance to Aircall, to believe that Aircall does not Process Personal Data in compliance with this DPA or the Applicable Data Protection Laws or that a Data Breach has occurred; or

b) The audit is formally requested by Customer's data protection authority; or

c) Applicable Data Protection Laws provide Customer with a direct audit right.

8.2. Audit frequency. The Customer shall conduct the audit at maximum once in any twelve month period, unless Applicable Data Protection Laws require more frequent audits.

8.3. Notice. The Customer shall provide at least thirty days advance notice of any audit unless mandatory Data Protection Law or a competent data protection authority requires shorter notice. The frequency and scope of any audits shall be mutually agreed between the parties acting reasonably and in good faith.

8.4. Cost of Audits. Each Party shall bear its costs of audits hereunder.

9. RETURN AND DELETION OF CUSTOMER'S DATA

9.1. Return (export) right and deletion. Upon the termination of the Agreement, Aircall will permit the Customer to export the Personal Data Processed under this DPA, at its expense, in accordance with the capabilities of the Service, within the period of thirty (30) days following such termination. After the expiry of such period, Aircall will delete all Personal Data stored or Processed by Aircall exclusively on behalf of the Customer and their copies, unless an applicable law requires storage of the personal data. The Customer expressly consents to such deletion and acknowledges that following the period stated in the first sentence of this Section, Aircall shall not be able to facilitate any export of the Personal Data to the Customer, as such Personal Data shall be either deleted or archived by Aircall as a Data Controller for the purpose(s) and for the period(s) stated in Aircall's Privacy Policy.

10. TERM AND AMENDMENTS

10.1 Commencement and previous agreements. This DPA becomes effective the date on which Customer accepted this DPA and replaces, as of the same date, any previously applicable data processing terms governing the Processing of Personal Data by Aircall on behalf of the Customer.

10.2. Duration. This DPA will remain in force as long as the Agreement.

10.3. Amendments. The customer explicitly acknowledges and agrees that this DPA may be amended in the same way as agreed by the parties for amendments of the Agreement, including Aircall's right to update the terms of the Agreement, any of its policies and this DPA from time to time, as decided by Aircall in its sole discretion, subject to notice to Customer at the Admin User Email Address.

11. LIABILITY

11.1. Aircall's aggregate liability. Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Affiliates and Aircall, whether in contract, tort (including negligence) or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement (or the section of the Agreement which addresses the exclusion and limitation of liability even if it

does not have that heading), and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together.

11.2. Liability towards Customer's Affiliates. For the avoidance of doubt, Aircall and its Affiliates' total liability for all claims from Customer and all of its Affiliates arising out of or related to the Agreement and all Data Processing Agreements whether in contract, tort (including negligence) or under any other theory of liability shall apply in the aggregate for all claims under both the Agreement and the Data Processing Agreements established under the Agreement or otherwise concluded between Aircall and the Customer and/or any Affiliate, and, in particular, shall not be understood to apply individually and severally to Customer and/or to any Affiliate that is a contractual party to, or otherwise entitled to claim under, any such Data Processing Agreement.

12. GOVERNING LAW AND JURISDICTION

12.1. Governing law. Without prejudice to mandatory application of Applicable Data Protection Laws, and respecting their potential mandatory prevalence, this DPA shall be governed by and construed in accordance with the laws of the country or territory stipulated for this purpose in the Agreement and each of the Parties agrees to submit to the choice of jurisdiction as stipulated in the Agreement in respect of any claim or matter arising under or related to this DPA.

12.2. Dispute resolution. In order to resolve amicably any dispute that may arise with respect to the interpretation, the performance and/or the termination of this DPA, the Parties agree to negotiate after the receipt of a notice by one of the Parties, with the intent to solve any dispute in an amicable way. Failing for the parties to reach an amicable settlement by signing a settlement agreement within thirty (30) days following the notification by a party of the existence of the dispute and making an express reference to this provision, the Parties shall submit their dispute to the relevant court that will have jurisdiction to settle the dispute.

Exhibit A

Description of the Processing

Aircall is authorised to process, on behalf of the Customer, the necessary personal data for providing Aircall product and related services.

The purposes of the Processing are:

1. Provision of Aircall product and services – Processing activities include:

- Operation of Aircall's infrastructure necessary for the processing of inbound and outbound calls and for secure and high-quality running of the platform.

- Personal data are switched between PSTN and VoIP, stored on Aircall's backend, processed for visualization and personal setting and monitored for potential errors.

- Analysing data on how the platform is used by users to provide statistics on the dashboard.

- Creation and maintenance of user accounts, coordination of allocation of phone numbers to users.

- Client identity check where required under local laws for provision of tel. numbers and where applicable creation of identity validation stamp to be used for future number procurement in the same location.

- Call routing, (manual) analysis of state of calls (from logs) for quality assurance and fixing issues.

- Analysing data pulled from API regarding crashes and bugs to assist resolving issues.

2. Integration of Aircall product with other tools – Processing activity:

- Sharing customer personal data with integration partners in case that the customer installs integration with the particular tool and authorizes the tool to access customer's data processed by Aircall and/or authorizes Aircall to access customer's data processed in the respective tool.

- Personal data will be transferred from Aircall to the respective tool provider and vice versa. Aircall's processing of personal data on behalf of the customer is limited to the processing performed in the Aircall environment.

The nature of operations carried out on the Personal Data is:

- Collection or recording of the Personal Data;

- Hosting or conservation of the Personal Data;

- Use of the Personal Data;

- Communication of the Personal Data by transmission, diffusion or any other way; and

- Deletion or destruction of the Personal Data.

Categories of Data Subjects

- Employees, agents and representatives of Customer
- Users' contacts and other individuals involved in communication via Aircall Call/SMS recipients, caller, sender

Types of Personal Data

- Customer account data (where the customer is a legal person, this data may also include customer representative data) – Customer contact name, Customer phone number, Customer contact email, Customer Aircall ID, Customer (legal) name, Customer tax number, Customer business address, Customer other data (contract details - pricing plan, additional terms, date & time of subscription, order form etc.;
- Customer contact data (from contact list) – Contact name, Contact tel. number, Contact owner, Contact picture;
- Information about user - User's ID, User 's metrics (first call, first log in, last call, last log in, %missed calls, number of calls answered), User User's IP address, User's role (user, admin), User's name, User's numbers, User's device information, User's availability status (history), User's location, User's contact book (retrieved from user's device);
- Call/SMS content – Call recordings, Voicemails, SMS, voice transcriptions; which may contain special categories of personal data;
- Call/SMS metadata – Call transfers, Call time, date, Call recipient number, Caller number, Call recipient prefix, Call duration, Call answered/missed, SMS time, date, Sender number, Recipient number, Aircall company, line and user involved;
- Additional call-related data - Call notes, Call tags, Call insight cards;
- Customer identity verification data (where the customer is a legal person, this data may also include customer representative data) – Customer physical address, Customer birthdate, Customer city of birth, Customer country of birth, Customer mother's name, Customer father's name, Customer nationality, Customer type of personal ID, Customer national ID number, Customer ID issuing authority, Customer ID issuing date, Customer representative job position, Customer's VAT Number / Fiscal code, Customer identity validation stamp.
- Customer provided documentation (where the customer is a legal person, this data may also include customer representative data) – Customer ID scan, Customer passport scan, Customer proof of address scan, Customer proof of business scan.

Period for which the personal data will be retained

- Personal Data Processed by Aircall exclusively on behalf of the Customer will be retained by default for a period agreed between Aircall and the Customer (based on Customer's pricing plan), unless the Customer gives Aircall an instruction to delete certain Personal Data sooner. Personal Data processed for provision of tel. numbers will be retained for the duration of the Agreement for provision of additional tel. numbers in the same location, unless instructed otherwise. Notwithstanding the above, Personal Data Processed by Aircall exclusively on behalf of the Customer will be deleted following the termination of the Agreement, i.e. at the moment of

expiration of the period for return and deletion of the Personal Data, as agreed by the Parties in this DPA.

- Personal Data Processed by Aircall also as a separate Data Controller will be retained for the retention period, as set forth in Aircall's Privacy Policy.

Exhibit B

Security Measures

As of the effective date of this DPA, Aircall, when Processing Personal Data on behalf of the Customer implemented and maintains the following technical and organizational security measures for the Processing of such Personal Data:

1. Information Security Program: Aircall will maintain reasonable information security program constructed around principles laid down in the information security industry standards. The information security program will cover topics such as : Policies and Procedures, Access Control, Business Continuity, HR Security, Network Infrastructure Security, Third-Party Security, Vulnerability Management, Vendor and Risk Management as well as Incident Response.

2. Security Certifications: Aircall will select an independent, qualified third-party auditor to conduct, at Aircall expense, at least annual audit of the security of the Services and environments, in accordance with SOC 2, Type II standards or its equivalent.

3. Physical Access Controls: Aircall shall take reasonable measures to prevent physical access, such as secured buildings and offices, to prevent unauthorized persons from gaining access to Personal Data.

4. System Access Controls: Aircall shall take reasonable measures to prevent Personal Data from being used without authorization. These controls shall vary based on the nature of the Processing undertaken and may include, among other controls, authentication via passwords and/or two-factors authentication, documented authorization processes, documented change management processes and/or, logging of access on several levels.

5. Data Access Controls: Aircall shall take reasonable measures to provide that Personal Data is accessible and manageable only by properly authorized staff, direct database query access is restricted and application access rights are established and enforced to ensure that persons entitled to use a data processing system only have access to the Personal Data to which they have the privilege of access; and, that Personal Data cannot be read, copied, modified or removed without authorization in the course of Processing.

6. Transmission Controls: Aircall shall take reasonable measures to ensure that it is possible to check and establish to which entities the transfer of Personal Data by means of data transmission facilities is envisaged so Personal Data cannot be read, copied, modified or removed without authorization during electronic transmission or transport. Personal Data is encrypted in transit over public networks when communicating with Aircall user interfaces (UIs) and application programming interface (APIs) via industry standard HTTPS/TLS (TLS 1.2 or higher). Personal Data is encrypted at rest by Aircall´s Subprocessor and managed services provider, Amazon Web Services Inc., via AES-256.

7. Input Controls: Aircall shall take reasonable measures to provide the ability to check and establish whether and by whom Personal Data has been entered into data processing systems, modified or removed.

8. Data Backup: Back-ups of the databases in the Service are taken on a regular basis, are secured, and encrypted to ensure that Personal Data is protected against accidental destruction or loss when hosted by Aircall.

9. Human Resources Security: Aircall employees undergo an extensive third-party background check prior to formal employment offers, wherever local regulations and employment standards permit. All Aircall employees must sign non-disclosure agreements

before gaining access to Personal Data. Every new employee must attend an information security and privacy training session during onboarding. After initial training, continuous training is provided which covers Aircall´s security policies, security best practices, and privacy principles.

10. Vendor Management: Aircall shall maintain a vendor management program to ensure that appropriate security controls are in place. Aircall periodically reviews each vendor (critical vendors are reviewed at least once a year) in light of Aircall's security and business continuity standards, including the type of access and classification of data being accessed (if any), controls necessary to protect data, and legal/regulatory requirements.

11. Platform Security Measures: Aircall splits its system into separate networks to better protect more sensitive data and to separate public services from internal services. Personal Data is only permitted to exist within the production network. Aircall shall perform penetration at least once per year using independent third-party entities to conduct application-level penetration tests. Security threats and vulnerabilities that are detected are prioritized, categorized, and resolved promptly. Aircall shall maintain, on the level of a good market standard, a bug bounty program with the aim to ethically discover security flaws in its system and to protect its system defences against sophisticated attacks, while inviting, incentivizing and, in a reasonable extent, responding to suggestions of independent security researchers.

12. Business Continuity: Aircall shall maintain and operate a Business Continuity and Disaster Recovery system based on best practices with the objective of providing reliability and availability to the operational phone systems and effective recovery in case of a disruptive event. Aircall recovery strategies are tested at least annually.

13. Data Center Security: Aircall hosts Personal Data primarily in AWS data centers that have been certified as ISO 27001, PCI DSS Service Provider Level 1, and/or SOC2 compliant. AWS infrastructure services include backup power, HVAC systems, and fire suppression equipment to help protect servers and ultimately your data. AWS on-site security includes a number of features, such as, security guards, fencing, securing feeds, intrusion detection technology, and other security measures. More details on AWS controls can be found at: https://aws.amazon.com/security