DATA PROCESSING AGREEMENT

This Data Processing Agreement was last updated on July 22, 2021. A record of the previous version of the Data Processing Agreement can be found here.

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 (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, the definition set forth by the Applicable Data Protection Laws shall apply instead of the definition ascribed by the GDPR.

"*Applicable Data Protection Laws*" means all data protection laws and regulations applicable to the Processing of Personal Data under the Agreement and this DPA, which may, depending on the circumstances, include the GDPR and/or HIPAA, as defined below.

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

"*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.

11-15 rue Saint Georges
75009 Paris – France
N° RCS PARIS 807 437 595

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.

"Standard Contractual Clauses" means the agreement executed if necessary pursuant to the European Commission's decision of 5 February 2010 on Standard Contractual Clauses for the transfer of Personal Data to processors established outside of the European Economic Area which do not ensure an adequate level of data protection.

"*Sub-processor*" means any subcontractor engaged by Aircall to Process all or part of the Personal Data for Aircall on behalf of the Customer.

1. APPLICATION OF DATA PROTECTION LAWS AND THE TERMS

1.1 **Applicable Data Protection Laws Compliance**. The Customer hereby represents that this DPA complies, to its reasonable knowledge, with Applicable Data Protection Laws and contains all provisions required by such laws.

1.2 **Applicability of GDPR.** 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. To the extent GDPR applies to the Processing of Personal Data under this DPA, the Customer acts as a Data Controller and Aircall acts as a Data Processor. The parties acknowledge that regardless of whether GDPR applies to the Processing of Personal Data under this DPA**,** other data protection laws may also apply to the Processing of Personal Data.

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.

1.4 **The terms.** Except to the extent this DPA states otherwise, the terms of this DPA will apply irrespective of whether the Processing of Personal Data under this DPA is subject to GDPR and/or other data protection laws. 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

1.5 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.

1.6 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 GDPR applies to the Processing of Personal Data under this DPA, the Customer, the Customer is, thus, liable complying with its obligations as Data Controller under all applicable laws and regulations, including informing the Data Subjects about the Processing of their Personal Data under this DPA, obtaining their consent, if necessary, and ensuring that it has the authority to use the Personal Data in accordance with the purposes defined herein.

1.7 Aircall's Processing of Personal Data. Aircall shall only Process Personal Data on behalf of and in accordance with Customer's documented instructions. 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/. With respect to U.S. Aircall customers, 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.

1.8 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, relevant Order Form and instructions provided via configuration tools incorporated in Aircall's platform 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.

1.9 Obligations of Aircall. 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 and/or applicable Order Forms;

b) Informs immediately the Customer if 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 Data Controller 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) 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 Article 28 of the GDPR, 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 Security 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.

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 inform the Data Subjects with the information on the processing of their Personal Data.

4.2. Exercise of data subjects' rights. 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 Data Controller) 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:

a) Notify the Customer via email sent to the email address associated with the Customer's Account 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.

5. SUB-PROCESSORS

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

5.2. General authorization. By executing the DPA, the Customer further grants Aircall with a general authorization to engage other Sub-processors, add or replace the Sub-processors in the list. In case the list of Sub-processors is modified by Aircall, Customer will be informed of any intended changes via email address associated with the Customer's Account. This information will clearly indicate which processing activities are being subcontracted out, the name and contact details of the sub-processor and the dates of the subcontract.

5.3. Objections. To the extent GDPR applies to the Processing of Personal Data under this DPA, 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 Sub-processors. 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 Sub-processor, it shall do so by way of a contract which imposes on the Sub-processor the same obligations as the ones imposed on Aircall under this DPA. Aircall shall ensure that the Sub-processor complies with the obligations to which the data processor is subject pursuant to this DPA and Applicable Data Protection Laws.

5.5. Sub-processor agreements. To the extent GDPR applies to the Processing of Personal Data under this DPA, Aircall shall provide, at the Controller's request, a copy of such a Sub-processor agreement and subsequent amendments to the Customer.

5.6. Liability. To the extent GDPR applies to the Processing of Personal Data under this DPA, Aircall shall be liable towards the Customer for the acts and omissions of its Sub-processors to the same extent Aircall would be directly liable if performing the Services of each Sub-processor directly under the terms of this DPA.

6. TRANSFERS OF EU PERSONAL DATA

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

6.2. Standard Contractual Clauses. The parties agree that the Standard Contractual Clauses set out as Exhibit C will apply in respect of Personal Data transferred from the European Economic Area (EEA) to a third country outside the EEA during the Processing of Personal Data, either directly by Aircall or via onward transfer to or by the Sub-processors, to any country or recipient: (i) not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the GDPR), or (ii) not covered by a suitable framework recognized by the relevant authorities or courts as providing an adequate level of protection for personal data.

6.3. Conflict. In the event of any conflict or inconsistency between this DPA and the Standard Contract Clauses in Exhibit C, the Clauses shall prevail.

6.4. Additional Measures. The parties agree that the following measures will apply in case that Aircall receives a Regulatory Action consisting in a binding order from any public authority of a third country described in Section 6.2 hereof for disclosure of Personal Data, whereby for these situations, this Section 6.4 prevails over the procedure agreed by the parties in Section 4.3 hereof:

a) Aircall shall:

a. Inform the requesting public authority of the incompatibility of the Regulatory Action with the safeguards contained in the DPA and the resulting conflict of obligations for Aircall;
b. Notify the Customer simultaneously and as soon as possible;
c. Review the legality of such Regulatory Action, including whether it remains within the powers granted to the requesting public authority;
d. Challenge the Regulatory Action if, after a careful assessment, Aircall concludes that there are grounds under the law of the country of destination to do so;
e. When challenging the Regulatory Action, Aircall shall seek interim measures to suspend the effects of the order until the court has decided on the merits;
f. Not disclose the Personal Data requested until required to do so under the applicable procedural rules; and
g. Disclose the minimum amount of information permissible when responding to the Regulatory Action, based on a reasonable interpretation of the order;

b) The Customer or its independent third-party auditor may conduct audit or inspection of the data processing facilities of Aircall, on-site and/or remotely, to verify if Personal Data was disclosed and under which conditions; and
c) Each party is entitled to unilaterally terminate this DPA and the Agreement in good will with immediate effect.

7. DATA BREACHES

7.1. Notification. Aircall will notify Customer of any data breach concerning Personal Data, which is likely to result in a risk to the rights and freedoms of the Data Subjects ("**Data Breach**") promptly after detection of such Data Breach by Aircall, no later than 24 hours after such detection. The notification shall be carried out via email sent to the email address associated with the Customer's Account.

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. 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. Following such period, Aircall will delete all Personal Data stored or Processed by Aircall exclusively on behalf of the Customer and their copies, unless EU or Member State law requires storage of the personal data. The Customer expressly consents to such deletion.

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 into 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, subject to notice to Customer at the email address associated with the Customer's Account, as decided by Aircall in its sole discretion.

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 DPAs 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 all DPAs established under the Agreement, including by Customer and all Affiliates, 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 DPA.

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 PSNT 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 agents to provide statistics on the dashboard.
- Creation and maintenance of user accounts, coordination of allocation of phone numbers to users.
- 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
- Agents' contacts and other individuals involved in communication via Aircall - Call/SMS recipients, caller, sender

Types of Personal Data

- Customer's account data – Customer contact (representative) name, Customer contact (representative) email, Customer (company) Aircall ID, Customer (company) name, Customer (company) tax number, Customer (company) physical address, Customer (company) other data (contract details - pricing plan, additional terms, date & time of subscription, order form etc.;

- Customer's contact data (from contact list) – Contact name, Contact tel. number, Contact owner, Contact picture;

- Information about agent - Agent's ID, Agent's metrics (first call, first log in, last call, last log in, %missed calls, number of calls answered), Agent's IP address, Agent's role (user, admin), Agent's name, Agent's numbers, Agent's device information, Agent's availability status (history), Agent's location, Agent's contact book (retrieved from agent's device);

- Call/SMS content – Call recordings, Voicemails, SMS; 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 agent involved;

- Call data - other - Call notes, Call tags, Call insight cards;

- Customer's scanned documents – Agent's ID scan, Agent's passport scan.

`

Exhibit B

Security Standards

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 (**"Security Standards"**):

1. **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.

2. **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.

3. **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.

4. **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 Service Data cannot be read, copied, modified or removed without authorization during electronic transmission or transport.

5. **Input Controls:** Aircall shall take reasonable measures to provide that it is possible to check and establish whether and by whom Service Data has been entered into data processing systems, modified or removed**.** Aircall shall take reasonable measures to ensure that (i) the Personal Data source is under the control of the Customer; and (ii) Personal Data is integrated into the Service is managed by secured file transfer from the Customer.

6. **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.

EXHIBIT C
STANDARD CONTRACTUAL CLAUSES

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

The entity identified as "Customer" in the DPA

(the data **exporter**)

And

The entity identified as "Aircall" in the DPA

(the data **importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i),

Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

  (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

  (ii) any accidental or unauthorised access, and

  (iii) any request received directly from the data subjects without responding to that

request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data

exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively

process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

Appendix 1 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

Data Exporter

The data exporter is the entity identified as “Customer” in the DPA.

Data Importer

The data exporter is the entity identified as “Aircall” in the DPA.

Data Subjects

The personal data transferred concern the categories of data subjects identified in Exhibit A of the DPA.

Categories of Data

The personal data transferred concern the categories of data identified in Exhibit A of the DPA.

Processing Operations

The personal data transferred concern the processing operations identified in Exhibit A of the DPA.

Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Data importer will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to the Aircall Services, as described in Exhibit B of the DPA.