DATA PROCESSING AGREEMENT

This Data Processing Agreement was last updated on September 17, 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.

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

"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.

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 decision of the Commission (EU) 2021/914 of 4 June 2021 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, 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/. 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, 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.

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, as required by article 32 of the GDPR, 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, to the extent legally permitted, 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 legally 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, to the extent legally permitted, 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 by giving written notice to the other Party.

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.

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.

  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 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 46(1) and (2)(c) of Regulation (EU) 2016/676 the Commission has adopted the Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries

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.

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add

[1] *Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.*

other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations

provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 - Optional

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE TWO: Transfer controller to processor

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under

Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter"personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data

for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[2] (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefiting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non- compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and

---

[2] *The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.*

shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub- processors at least [Specify time period] in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[3] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub- processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

[3] *This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.*

Data subject rights

MODULE TWO: Transfer controller to processor

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

MODULE TWO: Transfer controller to processor

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

MODULE TWO: Transfer controller to processor

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

MODULE TWO: Transfer controller to processor

(a) Where the data exporter is established in an EU Member State: The supervisory authority with

responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE TWO: Transfer controller to processor

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward

transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[4];

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three: , if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

---

4 *As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.*

Clause 15

Obligations of the data importer in case of access by public authorities

MODULE TWO: Transfer controller to processor

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When

challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data

exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

MODULE TWO: Transfer controller to processor

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of France.

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of France.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX 1

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

Data exporter(s):

Name: the entity identified as "Customer" in the Agreement

Address: identified in the Agreement

Contact details: email address associated with the Customer's Account, sa identified in the Agreement

Activities relevant to the data transferred under these Clauses: identified in the list of Sub-processors (Section 5.1 of the DPA)

Signature and date: detailed in the Agreement

Role (controller/processor): controller

Data importer(s):

Name: the entity defined as "Aircall" in the Agreement

Address: identified in the Agreement

Contact details: privacy@aircall.io

Activities relevant to the data transferred under these Clauses: identified in the list of Sub-processors (Section 5.1 of the DPA)

Signature and date: detailed in the Agreement

Role (controller/processor): processor

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred: detailed in Exhibit A of the DPA

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.*

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

Nature of the processing: detailed in Exhibit A of the DPA

Purpose(s) of the data transfer and further processing: detailed in Exhibit A of the DPA

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: detailed in Exhibit A of the DPA

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: identified in the list of Sub-processors (Section 5.1 of the DPA)

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

Competent supervisory authority/ies in accordance with Clause 13: Commission nationale de l'informatique et des libertés (CNIL)

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE TWO: Transfer controller to processor

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.

ANNEX III

LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

The Data exporter has authorised the use of the sub-processors detailed in Section 5.1 of the DPA and the list of Sub-processors referred to therein.