

DATA PROCESSING AGREEMENT

This Data Processing Agreement (“DPA”, “Agreement”) forms part of the master agreement between Subscriber and Lucas Loureiro Carvalho Suporte Tecnico ME. to reflect the parties’ agreement for the provision of the Processor Services (as amended from time to time) and processing of Subscriber’s Personal Data in accordance with the requirements of the Data Protection Legislation.

This Data Processing Agreement will be effective from the Effective Date.

If you are accepting these Data Processing Agreement on behalf of Subscriber, you warrant that: (a) you have full legal authority to bind Subscriber to this Data Processing Agreement; (b) you have read and understand this Data Processing Agreement; and (c) you agree, on behalf of Subscriber, to this Data Processing Agreement. If you do not have the legal authority to bind Subscriber, please do not accept this Data Processing Agreement.

APPLICATION OF THIS DPA

This DPA will only apply to the extent that the Data Protection Legislation applies to the processing of Subscriber’s Personal Data, including if:

- (a) The processing is in the context of the activities of an establishment of the Subscriber in the EEA; and/or
- (b) Offering services to data subjects who are in the EEA

This DPA shall not replace any previously applicable agreements relating to their subject matter (including any data processing amendment or data processing addendum relating to the Processor Services)

DEFINITIONS AND INTERPRETATION

“JivoChat” means the Lucas Loureiro Carvalho Suporte Tecnico ME., Rua Neves Armond, 140, Sala 301, Praia Do Suá. Vitória, ES/Brazil, that is a party to this DPA and its Affiliates engaged in the Processing of Personal Data.

“Criminal offence data” means Personal data relating to criminal convictions and offences.

“Subscriber Personal Data” means personal data that is processed by JivoChat on behalf of Subscriber as part of JivoChat provision of the Processor Services.

“Data Incident” means a breach of JivoChat security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Subscriber’s Personal Data on systems managed by or otherwise controlled by JivoChat. “Data Incidents” will not include unsuccessful attempts or activities that do not compromise the security of Subscriber Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

“Data Protection Legislation” means, as applicable: (a) the GDPR; (b) the Swiss Federal Act on Data Protection (FADP), UK GDPR, UK Data Protection Act 2018 and the California Consumer Privacy Act of United States

“Effective Date” means, as applicable: the date on which Subscriber signed this DPA.

“GDPR” means 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, and repealing Directive 95/46/EC.

“Notification Email Address” means the email address (if any) designated by Subscriber, via the user interface of the Processor Services or such other means provided by JivoChat, to receive certain notifications from JivoChat relating to this Data Processing Agreement.

“Personal Data” means any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic cultural or social identity;

“Processing of personal data” and “Processor Services“ means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction (“Process”, “Processes” and “Processed” shall have the same meaning).

“Security measures” means measures to protect personal data against accidental or unlawful destruction or accidental loss, alternation, unauthorized disclosure or access and against all other unlawful forms of processing as described in the document (or the applicable part dependent on what Services Subscriber purchases from JivoChat), as updated from time to time, and accessible via the link in Appendix 2 to the Standard Contract Clauses.

“Special category data” means personal data consisting of information as to the racial or ethnic origin of the data subject, his political opinions, his religious beliefs or other beliefs of a similar nature, whether he is a member of a trade union, his physical or mental health or condition, his sexual life. The special category specifically includes genetic data, and biometric data where processed to uniquely identify an individual.

“Sub-processors” means third parties authorized by JivoChat to have logical access to and process Subscriber Personal Data in order to provide parts of the Processor Services and any related technical support.

“Subscriber” – JivoChat enables the Subscribers (“Subscriber” or “you”) to communicate with their customers (the “Customers”) in real time by means of live chat (the “JivoChatService”)

“Term” means the period from the Effective Date until the end of JivoChat provision of the Processor Services to Subscriber under the Agreement.

The terms “Data controller”, “Data subject”, “Personal data”, “Processing”, “Data processor” and “Supervisory authority” as used in this DPA have the meanings given in the Data Protection Legislation.

Effective Date: [29.06.2022]

The Parties,

- **Lucas Loureiro Carvalho Suporte Tecnico ME.**, with its registered address at Rua Neves Armond, 140, Sala 301, Praia Do Suá, Vitória, ES/Brazil(“JivoChat”);
- **[Coeln Concept GmbH]**, a company having its principle place of business in [Uhlstraße 19 - 23, D-50321 Brühl, Germany], hereby duly represented by [Dr. Thomas Müller], (the “Subscriber”);

hereinafter collectively referred to as “Parties” and individually “Party”,

having regard to the fact that,

- the Subscriber has access to the personal data, within the meaning of the GDPR, of the Subscriber’s various customers (“Customer(s)”) who reside in the EU and communicate and transmit personal data to the Subscriber through JivoChatService (“Data Subjects”);
- Subscriber is the controller and maintains control over the Data Subjects’ personal data, and as such the Subscriber has determined the purpose of and the means for the processing of personal data as governed by the JivoChat terms and conditions and the Data Processing Agreement referred to herein;
- JivoChat has undertaken to comply with this data processing agreement (the “Data Processing Agreement”) and to abide by the security obligations and all other aspects of the DataProtection Legislation;
- the Subscriber is hereby deemed to be the responsible party within the meaning of Article 24 of the GDPR;
- Subscriber shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Subscriber acquired Personal Data;
- JivoChat is hereby deemed to be the processor within the meaning of Article 28 of the GDPR;
- the Parties, having regard also to the provisions of Article 30 of the GDPR, wish to lay down their rights and duties in writing in this Data Processing Agreement,

have agreed as follows,

1 PROCESSING OBJECTIVES

1.1. JivoChat will process Data Subjects’ personal data only to the extent strictly necessary for the purpose of providing the services in accordance with JivoChat Terms of Service and this Data Processing Agreement.

1.2. By entering into this Data Processing Agreement, Subscriber instructs JivoChat to process Subscriber Personal Data only in accordance with applicable law: (a) to provide the Processor Services and any related technical support; (b) as further specified via Subscriber’s use of the Processor Services (including in the settings and other functionality of the Processor Services) and any related technical support; (c) as documented in this Data Processing Agreement; and (d) as further documented in any other written instructions given by Subscriber and acknowledged by JivoChat as constituting instructions for purposes of this Data Processing Agreement. Instructions of Personal Data Processing are described in JivoChat Terms of Service.

1.3 Subscriber’s Personal Data may include the types of personal data described below:

- personal details;
- contact details;
- Device and connectivity information such as IP (Internet Protocol) address, browser type and version;
- location country, city, state and region;
- online identifiers;
- device identifiers;

1.4 Subscriber will not assist or permit any third party to, pass special category data or criminal offence data through the use of JivoChat applications. The subscriber is hereby notified, that any submission of special category data or criminal offence data by the Subscriber or data subjects about whom personal data is transferred to JivoChat in connection with the Processor Services by, at the direction of, or on

behalf of Subscriber, will be solely at Subscriber's own risk and responsibility and will be considered an occasional submission.

1.5 Subscriber Personal Data will concern the following categories of data subjects:
- data subjects about whom JivoChat collects personal data in its provision of the Processor Services.

1.6 JivoChat shall refrain from making use of the personal data for any purpose other than as specified by the Subscriber. The Subscriber will inform JivoChat of any such purposes which are not contemplated in this Data Processing Agreement.

1.7 All personal data processed on behalf of the Subscriber shall remain the property of the Subscriber and/or the relevant Data Subjects.

2 JIVOCHAT'S OBLIGATIONS

2.1 JivoChat shall warrant compliance with the Data Protection Legislation, including laws and regulations governing the protection of personal data, such as the GDPR.

2.2 Personnel

2.2.1. JivoChat shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and are subject to obligations of confidentiality as described in Appendix 2 to the Standard Contract Clauses and such obligations survive the termination of that persons' engagement with JivoChat.

2.2.2. JivoChat shall ensure that JivoChat Group's access to Personal Data is limited to those personnel who require such access to perform the Agreement.

2.3 Data Security

2.3.1. JivoChat shall maintain administrative, physical and technical safeguards for protection of the security, confidentiality and integrity of Personal Data, such measures are described in Appendix 2 to the Standard Contract Clauses.

2.3.2. JivoChatSecurity Measures. JivoChat will implement and maintain technical, physical and organizational measures to protect confidentiality and integrity of Subscriber Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access as described in Appendix 2 to the Standard Contract Clauses (the "Security Measures"). As described in Appendix 2 to the Standard Contract Clauses, the Security Measures include measures: (a) to help ensure the ongoing confidentiality, integrity, availability and resilience of JivoChat systems and services; (b) to help restore timely access to personal data following an incident; and (c) for regular testing of effectiveness. JivoChat may update or modify the Security Measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Processor Services.

2.3.3. Security Compliance by JivoChatStaff. JivoChat will take appropriate steps to ensure compliance with the Security Measures by its employees, contractors and Sub-processors to the extent applicable to their scope of performance, including ensuring that all persons authorized to process Subscriber Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality as described in Appendix 2 to the Standard Contract Clauses.

2.3.4. JivoChatSecurity Assistance. Subscriber agrees that JivoChat will assist Subscriber in ensuring compliance with any obligations in respect of security of personal data and personal data breaches, including (if applicable) Subscriber's obligations pursuant to Articles 32 to 34 (inclusive) of the GDPR, by:

(a) implementing and maintaining the Security Measures in accordance with the Appendix 2 to the Standard Contract Clauses;

(b) complying with the terms of Section 6.5 (Data Incidents).

3 INTERNATIONAL DATA TRANSFERS

3.1 Data Storage and Processing Facilities. JivoChat will store and process Subscriber Personal Data in the European Union and the Russian Federation.

3.2 The European Commission has approved the use of standard contract clauses as a means of ensuring adequate protection when transferring data outside of the EEA. By incorporating standard contract clauses into a contract established between the parties transferring data, personal data can be protected when transferred outside the EEA to countries which have not been deemed by the European Commission to adequately protect personal data. The security of data and the data subject rights under GDPR for the data processing activities in United States are protected by JivoChat by the appropriate safeguards under article 46 GDPR, as described in the Schedule 1.

3.3 The representative established in the European Union on behalf of Lucas Loureiro Carvalho Suporte Tecnico ME. is Elena Riazanova with her registered address at C/ Cullera 11, 3C Madrid, Spain and her contact email info@security-trend.co.uk.

4 ALLOCATION OF RESPONSIBILITY

4.1 JivoChat shall only be responsible for processing the personal data under this Data Processing Agreement, in accordance with the Subscriber's instructions. JivoChat is explicitly not responsible for other processing of personal data, including but not limited to processing for purposes that are not reported by the Subscriber to JivoChat, and processing by third parties and / or for other purposes.

4.2 Subscriber represents and warrants that it has express consent and/or a legal basis to process the relevant personal data. Furthermore, the Subscriber represents and warrants that the contents are not unlawful and do not infringe any rights of a third party. In this context, the Subscriber indemnifies JivoChat of all claims and actions of third parties related to the processing of personal data without express consent and/or legal basis under this Data Processing Agreement.

5 ENGAGING OF THIRD PARTIES OR SUBCONTRACTORS

5.1 Consent to Sub-processor Engagement. Subscriber generally authorizes that JivoChat and its Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Service. JivoChat and JivoAffiliates have entered into a written agreement with each Sub-processor containing data protection obligations not less protective than those in this DPA with respect to the protection of Subscriber Data to the extent applicable to the nature of the Services provided by such Sub-processor.

5.2 JivoChat makes available in Terms of Service to Subscriber the current list of Sub-processors for its Services.

5.3 When engaging any Sub-processor, JivoChat will:

(a) ensure via a written contract that;

(i) the Sub-processor only accesses and uses Subscriber Personal Data to the extent required to perform the obligations subcontracted to it, and does so in accordance with the Agreement (including this DPA); and;

- (ii) The data protection obligations set out in Article 28(3) of the GDPR are imposed on the Sub-processor;
- b) inform to Subscriber about change Sub-processors.

5.4 **Objection Right** to New Sub-processors. When any new Sub-processor is engaged during the Term, JivoChat will, at least two (2) weeks before the new Sub-processor processes any Subscriber Personal Data, notify subscriber via email and specify the new Sub-processor entity. Subscriber may object to any new Sub-processor by notifying JivoChat promptly in writing within five (5) business days. In the event Subscriber objects to a new Sub-processor, JivoChat will make commercially reasonable efforts to make available to Subscriber a change and avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening the Subscriber. If JivoChat is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Subscriber may terminate this DPA via a written notification to JivoChat.

6 DUTY TO REPORT

6.1 Data incidents:

6.1.1 Incident Notification. If JivoChat becomes aware of a Data Incident, JivoChat will: (a) notify Subscriber of the Data Incident promptly (within 48 hours) and without undue delay; and (b) promptly take reasonable steps to minimize harm and secure Subscriber Personal Data.

6.1.2 Details of Data Incident. Notifications will describe, to the extent possible, details of the Data Incident, including steps taken to mitigate the potential risks and steps JivoChat recommends Subscriber take to address the Data Incident.

6.1.3 Delivery of Notification. JivoChat will deliver its notification of any Data Incident to the Notification Email Address or, at JivoChat discretion (including if Subscriber has not provided a Notification Email Address), by other direct communication (for example, by phone call or an in-person meeting). Subscriber is solely responsible for providing the Notification Email Address and ensuring that the Notification Email Address is current and valid.

6.1.4 Third Party Notifications. Subscriber is solely responsible for complying with breach notification laws applicable to Subscriber and fulfilling any third party notification obligations related to any Data Incident.

7 SECURITY

7.1 JivoChat will endeavor to take reasonable technical and organizational measures against loss or any form of unlawful processing (such as unauthorized disclosure, deterioration, alteration or disclosure of personal data) in connection with the performance of processing personal data under this Data Processing Agreement as described in Appendix 2 to the Standard Contract Clauses (the "Security Measures").

7.2 As described in Appendix 2 to the Standard Contract Clauses, the Security Measures include measures: (a) to help ensure the ongoing confidentiality, integrity, availability and resilience of JivoChat systems and services; (b) to help restore timely access to personal data following an incident; and (c) for regular testing of effectiveness. JivoChat may update or modify the Security Measures from time to time, provided that such updates and modifications do not result in the degradation of the overall security of the Processor Services.

8 RIGHTS OF DATA SUBJECTS

8.1 To the extent Subscriber, in its use or receipt of the Services, does not have the ability to correct, amend, block or delete Personal Data, as required by Data Protection Legislation, JivoChat will (taking into account the nature of the processing of Subscriber's Personal Data and, if applicable, Article 11 of the GDPR) assist Subscriber in fulfilling any obligation of Subscriber to respond to requests by data subjects, including (if applicable) Subscriber's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR, by providing the functionality of the Processor Services.

8.2 JivoChat shall, to the extent legally permitted, promptly notify Subscriber if it receives a request from a Data Subject for access to, correction, amendment, restriction, deletion or exercising any other rights under the GDPR of that person's Personal Data. JivoChat shall not respond to any such Data Subject request without Subscriber's prior written consent except to confirm that the request relates to Subscriber. JivoChat shall provide Subscriber with cooperation and assistance in relation to handling of a Data Subject's request for access to that person's Personal Data or exercising any other rights under the GDPR, to the extent legally permitted and to the extent Subscriber does not have access to such Personal Data through its use or receipt of the Services.

9 AUDIT

9.1 In order to confirm compliance with this Data Processing Agreement, the Subscriber may conduct an audit, not more often than once per year, in relation to the processing of personal data by JivoChat by assigning an independent third party who shall be obliged to observe confidentiality in this regard. Any such audit will follow JivoChat's reasonable security requirements, and will not interfere unreasonably with JivoChat's business activities.

9.2 The costs of the audit will be borne by the Subscriber.

10 DURATION, DATA RETENTION AND TERMINATION

10.1 This Data Processing Agreement is entered into for the duration of the cooperation between the you and JivoChat.

10.2 The Subscriber's personal data retention criteria is the duration of the cooperation between you and JivoChat plus the legal obligation retention period required by the applicable legislation.

Lucas Loureiro Carvalho Suporte Tecnico ME.

[SUBSCRIBER]

____/____/____

Date

[29/06/2022

Date



Lucas Loureiro Carvalho

Name

[Dr. Thomas Müller]

Name

**Schedule 1 STANDARD CONTRACTUAL CLAUSES (CONTROLLER TO
PROCESSOR AND PROCESSOR TO PROCESSOR)**

STANDARD CONTRACTUAL CLAUSES

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 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) Clause 16(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

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 (4) (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 benefitting 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 noncompliance. 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 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.

MODULE THREE: Transfer processor to processor

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

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 controller, as communicated to the data importer by the data exporter, or 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 personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand 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.

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 rectify or erase 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 controller 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, they 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 subject. 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 or the controller. 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 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, without undue delay, the data exporter and, where appropriate and feasible, the controller 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 data breach, including 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 its controller so that the latter may in turn 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 set out 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 controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (6) (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 benefitting 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 of Regulation (EU) 2016/679;
- (iii) (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 or the controller 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 controller.
- (c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.
- (d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.
- (e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.
- (f) 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 shall, where appropriate, be carried out with reasonable notice.
- (g) 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

GENERAL WRITTEN AUTHORISATION

- (a) 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 five (5) business days 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.

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.

MODULE THREE: Transfer processor to processor

GENERAL WRITTEN AUTHORISATION The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 5 working days in advance, thereby giving the controller 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 controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), 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. 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 or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. 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

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.

MODULE THREE: Transfer processor to processor

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. 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 controller, as communicated by the data exporter.

Clause 11

Redress

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

MODULE THREE: Transfer processor 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 FOUR: Transfer processor to controller

(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) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party 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 under Regulation (EU) 2016/679.

(c) 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.

(d) The Parties agree that if one Party is held liable under paragraph (c), 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.

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

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor 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 subprocessor) 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

MODULE THREE: Transfer processor to processor

(a) 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.

(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

MODULE THREE: Transfer processor 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 (12);

(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). The data exporter shall forward the notification to the controller.

(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, 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 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.

Clause 15

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

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor 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.

The data exporter shall forward the notification to the controller.

(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.). The data exporter shall forward the information to the controller.

(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. The data exporter shall make the assessment available to the controller.

(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

(iv) 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 and the controller of such noncompliance. 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

MODULE THREE: Transfer processor 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 Germany.

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor 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 Germany.

(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 I

LIST OF PARTIES

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Data exporter(s): Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union


1. Name: Coeln Concept GmbH

Address: Uhlstraße 19-23, D-50321 Brühl, Germany

Contact person's name, position and contact details: Dr. Thomas Müller, managing director, +49 2232 50155-100, Uhlstraße 19-23, D-50321 Brühl, Germany

Activities relevant to the data transferred under these Clauses: Getting in contact with possible clients about our products.

Signature and date: 29.6.2022



Role (controller/processor): processor

Data importer(s):

Name: Lucas Loureiro Carvalho Suporte Tecnico ME.

Address: Rua Neves Armond, 140, Sala 301, Praia Do Suá. Vitória, ES/Brazil

Contact person's name, position and contact details: EU Representative Elena Riazanova

Activities relevant to the data transferred under these Clauses: Omnichannel business messenger built to connect with the website visitors via live chat, voice services, email, and mobile.

Signature and date:
.....

Role (controller/processor): Controller and processor

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Categories of data subjects whose personal data is transferred

- Subscriber's website visitors;
- Subscriber's customers;
- Subscriber's prospects;
- Other data subjects about whom JivoChat collects personal data in its provision of the Processor Services.

Categories of personal data transferred

- personal details;
- contact details;
- Device and connectivity information such as IP (Internet Protocol) address, browser type and version;
- location country, city, state and region;
- online identifiers;
- device identifiers;

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

N/A

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Infrequent

Nature of the processing

- to provide the Processor Services and any related technical support;
- as further specified via Subscriber's use of the Processor Services (including in the settings and other functionality of the Processor Services) and any related technical support;
- as documented in this Data Processing Agreement; and
- as further documented in any other written instructions given by Subscriber and acknowledged by JivoChat as constituting instructions for purposes of this Data Processing Agreement. Instructions of Personal Data Processing are described in JivoChatTerms of Service.

Purpose(s) of the data transfer and further processing

- to provide the Processor Services and any related technical support;
- as further specified via Subscriber's use of the Processor Services (including in the settings and other functionality of the Processor Services) and any related technical support;
- as documented in this Data Processing Agreement; and
- as further documented in any other written instructions given by Subscriber and acknowledged by JivoChat as constituting instructions for purposes of this Data Processing Agreement. Instructions of Personal Data Processing are described in JivoChatTerms of Service.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

During the contract duration plus any applicable legal requirements

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Hosting provider, during the contract duration plus any applicable legal requirements

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Identify the competent supervisory authority/ies in accordance with Clause 13

Supervisory authority of Ireland

ANNEX II

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

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

1. Data centers & Network Security

(a) Data Centers.

INFRASTRUCTURE

Data Importer uses OVH Cloud to store and analyze data, including infrastructure Europe (England) Region.

PHYSICAL SECURITY

Employee Data Center access. Physical data center access is provided only to approved employees. All employees who need data center access must first apply for access and provide a valid business justification. These requests are granted based on the principle of least privilege, where requests must specify to which layer of the data center the individual needs access, and are time-bound. Requests are reviewed and approved by authorized personnel, and access is revoked after the requested time expires. Once granted admittance, individuals are restricted to areas specified in their permissions.

Third-party data center access. Access is requested by approved OVNcloud employees, who must apply for third-party access and provide a valid business justification. These requests are granted based on the principle of least privilege, where requests must specify to which layer of the data center the individual needs access, and are time-bound. These requests are approved by authorized personnel, and access is revoked after request time expires. Once granted admittance, individuals are restricted to areas specified in their permissions. Anyone granted visitor badge access must present identification when arriving on site and are signed in and escorted by authorized staff.

MONITORING & LOGGING

Data Center access review. Access to data centers is regularly reviewed. Access is automatically revoked when an employee's record is terminated in OVNcloud's HR system. In addition, when an employee or contractor's access expires in accordance with the approved request duration, his or her access is revoked.

Data Center Access logs. Physical access to OVNcloud data centers is logged, monitored, and retained. OVNcloud correlates information gained from logical and physical monitoring systems to enhance security on an as-needed basis.

Data Center Access monitoring. Data centers are monitored by global Security Operations Centers, which are responsible for monitoring, triaging, and executing security programs. They provide 24/7 global support by managing and monitoring data center access activities, equipping local teams and other support teams to respond to security incidents by triaging, consulting, analyzing, and dispatching responses.

SURVEILLANCE & DETECTION

CCTV. Physical access points to server rooms are recorded by Closed Circuit Television Camera (CCTV). Images are retained according to legal and compliance requirements.

Data Center entry points. Physical access is controlled at building ingress points by professional security staff utilizing surveillance, detection systems, and other electronic means. Authorized staff utilize multi-factor authentication mechanisms to access data centers. Entrances to server rooms are secured with devices that sound alarms to initiate an incident response if the door is forced or held open.

Intrusion detection. Electronic intrusion detection systems are installed within the data layer to monitor, detect, and automatically alert appropriate personnel of security incidents. Ingress and egress points to server rooms are secured with devices that require each individual to provide multi-factor authentication before granting entry or exit. These devices will sound alarms if the door is forced open without authentication or held open. Door alarming devices are also configured to detect instances where an individual exits or enters a data layer without providing multi-factor authentication. Alarms are immediately dispatched to 24/7 OVNcloud Security Operations Centers for immediate logging, analysis, and response.

REDUNDANCY

Data centers are designed to anticipate and tolerate failure while maintaining service levels. In case of failure, automated processes move traffic away from the affected area. Core applications are deployed to an N+1 standard, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.

AVAILABILITY

OVNcloud has identified critical system components required to maintain the availability of our system and recover service in the event of outage. Critical system components are backed up across multiple, isolated locations known as Availability Zones. Each Availability Zone is engineered to operate independently with high reliability. Availability Zones are connected to enable you to easily architect applications that automatically fail-over between Availability Zones without interruption. Highly resilient systems, and therefore service availability, is a function of the system design. Through the use of Availability Zones and data replication, OVNcloud customers can achieve extremely short recovery time and recovery point objectives, as well as the highest levels of service availability.

BUSINESS CONTINUITY PLAN

The OVNcloud Business Continuity Plan outlines measures to avoid and lessen environmental disruptions. It includes operational details about steps to take before, during, and after an event. The Business Continuity Plan is supported by testing that includes simulations of different scenarios. During and after testing, OVNcloud documents people and process performance, corrective actions, and lessons learned with the aim of continuous improvement.

PANDEMIC RESPONSE

OVNcloud incorporates pandemic response policies and procedures into its disaster recovery planning to prepare to respond rapidly to infectious disease outbreak threats. Mitigation strategies include alternative staffing models to transfer critical processes to out-of-region resources, and activation of a crisis management plan to support critical business operations. Pandemic plans reference international health agencies and regulations, including points of contact for international agencies.

ASSET MANAGEMENT

OVNcloud assets are centrally managed through an inventory management system that stores and tracks owner, location, status, maintenance, and descriptive information for OVNcloud-owned assets. Following procurement, assets are scanned and tracked, and assets undergoing maintenance are checked and monitored for ownership, status, and resolution.

MEDIA DESTRUCTION

Media storage devices used to store customer data are classified by OVNcloud as Critical and treated accordingly, as high impact, throughout their life-cycles. OVNcloud has exacting standards on how to install, service, and eventually destroy the devices when they are no longer useful. When a storage device has reached the end of its useful life, OVNcloud decommissions media using techniques detailed in NIST 800-88. Media that stored customer data is not removed from OVNcloud control until it has been securely decommissioned.

OPERATIONAL SUPPORT SYSTEMS

Power. OVNcloud data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day. OVNcloud ensures data centers are equipped with back-up power supply to ensure power is available to maintain operations in the event of an electrical failure for critical and essential loads in the facility.

Climate and temperature. OVNcloud data centers use mechanisms to control climate and maintain an appropriate operating temperature for servers and other hardware to prevent overheating and reduce the possibility of service outages. Personnel and systems monitor and control temperature and humidity at appropriate levels.

FIRE DETECTION AND SUPPRESSION

Fire detection and suppression. OVNcloud data centers are equipped with automatic fire detection and suppression equipment. Fire detection systems utilize smoke detection sensors within networking, mechanical, and infrastructure spaces. These areas are also protected by suppression systems.

LEAKAGE DETECTION

In order to detect the presence of water leaks, OVNcloud equips data centers with functionality to detect the presence of water. If water is detected, mechanisms are in place to remove water in order to prevent any additional water damage.

INFRASTRUCTURE MAINTENANCE

Equipment maintenance. OVNcloud monitors and performs preventative maintenance of electrical and mechanical equipment to maintain the continued operability of systems within OVNcloud data centers. Equipment maintenance procedures are carried out by qualified persons and completed according to a documented maintenance schedule.

Environment management. OVNcloud monitors electrical and mechanical systems and equipment to enable immediate identification of issues. This is carried out by utilizing continuous audit tools and information provided through our Building Management and Electrical Monitoring Systems. Preventative maintenance is performed to maintain the continued operability of equipment.

GOVERNANCE & RISK

Data Center risk management. The OVNcloud Security Operations Center performs regular threat and vulnerability reviews of data centers. Ongoing assessment and mitigation of potential vulnerabilities is performed through data center risk assessment activities. This assessment is performed in addition to the enterprise-level risk assessment process used to identify and manage risks presented to the business as a whole. This process also takes regional regulatory and environmental risks into consideration.

Third-party security attestation. Third-party testing of OVNcloud data centers, as documented in our third-party reports, ensures OVNcloud has appropriately implemented security measures aligned to established rules needed to obtain security certifications. Depending on the compliance program and its requirements, external auditors may perform testing of media disposal, review security camera footage, observe entrances and hallways throughout a data center, test electronic access control devices, and examine data center equipment.

(b) Networks & Transmission.

Data Transmission. Data Importer's Datacenters are connected via private links protected by OVNcloud Network firewalls to provide secure data transfer. This is designed to protect the confidentiality, integrity and availability of the network and prevent data from being read, copied, altered or removed without authorization during electronic transfer.

Intrusion Detection. Intrusion detection is intended to prevent ongoing attack activities and provide adequate information to respond to incidents. JivoChat intrusion detection involves:

- (a) Employing intelligent detection controls at data entry points; and
- (b) Employing technologies that automatically remedy certain dangerous situations.

Data Breach Response. JivoChat monitors a variety of communication channels for security breaches, and Data Importer's security personnel will react promptly to known incidents.

External Attack Surface. Data Importer considers potential attack vectors and incorporates appropriate purpose built proprietary technologies into external facing systems.

Encryption Technologies. Data Importer uses HTTPS encryption (also referred to as SSL or TLS connection).

2. Personnel Security

JivoChat personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. Data Importer conducts reasonably appropriate background checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations.

Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, JivoChat confidentiality and privacy policies. Personnel are provided with security training. Personnel handling Customer Personal Data are required to complete additional requirements appropriate to their role. Data Importer's personnel will not process Customer Personal Data without authorization.