EXHIBIT B

DATA PROCESSING AGREEMENT

This Data Processing Agreement (the "DPA") constitutes a legally binding agreement between You (the "Customer", "You", "Your") and Us ("Whatfix", "Us", "We", "Our"). You are required to read this DPA carefully as this DPA forms an integral part of the Terms of Service available at https://whatfix.com/terms-services/ (the "Terms") and is applicable where We are the Processors of Your Personal Data. In the event of a conflict between this DPA and the Terms, this DPA shall prevail.

1. **Definitions**

Terms not specifically defined herein shall have the meaning ascribed thereto in the Terms.

In this DPA, the following terms shall have the following meanings:

"**CCPA**" shall mean the California Consumer Privacy Act of 2018, and any related regulations or guidance provided by the California Attorney General.

"Customer Content" means all data and materials created or provided by the Company to Whatfix for use in connection with the SaaS Services, including, without limitation, flows, text snippets, images, and videos

"**Controller**", "**Data Subject**", "**Personal Data Breach**", "**Processor**" and "**Process**" shall have the meaning given to them in the GDPR and, as applicable, the CCPA.
"**Data Protection Laws**" shall mean the data protection laws of the country in which You are established, including the GDPR, the CCPA, and any data protection laws applicable to You in connection with the Terms (including without limitation, the Data Protection Act 2018 if You are established in the United Kingdom).

"**GDPR**" shall mean the 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 (General Data Protection Regulation), and if You are established in the United Kingdom, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.

"**Model Clauses**" means the standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 (as amended or updated from time to time) and shared with this DPA as APPENDIX 2.

"**Parent Company**" refers to Quicko Technosoft Labs Private Ltd, an Indian company registered under the laws of India and having its registered office at 443, 2nd and 3rd Floor, 14th Main, 17th Cross, Sector - 4, HSR Layout, Bangalore - 560102, India

"**Personal Data**" shall mean any information relating to an identified or identifiable natural person as defined by GDPR, CCPA and any other applicable privacy regulation , that is Processed by Processor as part of providing the services to You as described in an Appendix.

2. **Scope and Responsibilities**

- This DPA applies to Processing of Personal Data forming part of Customer Content.
- Whatfix shall process Personal Data only on Your behalf and at all times only in accordance with this DPA, especially the respective Appendix. For the avoidance of doubt, Whatfix shall be the Processor and You shall be the Controller of the Personal Data.
- Within the scope of the Terms, each party shall be responsible for complying with its respective obligations as Controller and Processor under Data Protection Laws.

3. Term and Termination

- This DPA becomes effective upon signature. It shall continue to be in full force and effect as long as Whatfix is Processing Personal Data pursuant to the Terms and shall terminate automatically thereafter.
- Where amendments are required to ensure compliance of this DPA or an Appendix with Data Protection Laws, the parties shall make reasonable efforts to agree on such amendments upon your request. Where the parties are unable to agree upon such amendments, either party may terminate the Agreement with 90 days written notice to the other party.

4. Processing Instructions

- Whatfix will Process Personal Data in accordance with Your instructions. This DPA contains Your initial instructions to Whatfix. The parties agree that You may communicate any change in its initial instructions to Whatfix by way of amendment to this DPA.
- For the avoidance of doubt, any instructions that would lead to Processing outside the scope of this DPA (e.g. because a new Processing purpose is introduced) will require a prior agreement between the parties and, where applicable, shall be subject to the contract change procedure under the respective Agreement.
- Whatfix shall without undue delay inform You in writing if, in Whatfix reasonable opinion, an instruction infringes Data Protection Laws, and provide a detailed explanation of the reasons for its opinion in writing.

5. Processor Personnel

- Whatfix will restrict its personnel from Processing Personal Data without authorisation. Whatfix will impose appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection and data security.

6. Disclosure to Third Parties; Data Subjects Rights

- Whatfix will not disclose Personal Data to any government agency, court, or law enforcement except with Your written consent or as necessary to comply with applicable mandatory laws. If Whatfix is obliged to disclose Personal Data to a law enforcement agency Whatfix agrees to give You reasonable notice of the access request prior to granting such access, to allow You to seek a protective order or other appropriate remedy (provided that you seek any such order or remedy within the relevant time frame set out in the notice given by Whatfix to You). If such notice is legally prohibited, Whatfix will take reasonable measures to protect the Personal Data from undue disclosure as if it were Whatfix's own confidential information being requested and shall inform You promptly as soon as possible if and when such legal prohibition ceases to apply.
- In case You receive any request or communication from Data Subjects which relates to the Processing of Personal Data ("Request"), Whatfix shall reasonably provide You with full cooperation, information and assistance ("Assistance") in relation to any such Request where instructed by You.
- Where Whatfix receives a Request, Whatfix shall (i) not directly respond to such Request, (ii) forward the Request to You within five (5) business days of identifying the Request as being related to You and (iii) provide Assistance according to further instructions from You.

7. Technical and Organizational Measures

- Whatfix shall implement and maintain appropriate technical and organizational security measures to ensure that Personal Data is Processed according to this DPA, to provide Assistance and to protect Personal Data against a Personal Data Breach ("TOMs"). Such

measures shall include the measures outlined in Annex II.

8. Assistance with Data Protection Impact Assessment

- Where a Data Protection Impact Assessment ("DPIA") is required under applicable Data Protection Laws for the Processing of Personal Data, Whatfix shall provide upon request to You any information and assistance reasonably required for the DPIA and assistance for any communication with data protection authorities, where required, unless the requested information or assistance is not pertaining to Whatfix's obligations under this DPA.
- You shall pay Whatfix reasonable charges for providing the assistance in clause 7, to the extent that such assistance is not reasonably able to be accommodated within the normal provision of the Services.

9. Information Rights and Audit

- Whatfix shall, in accordance with Data Protection Laws, make available to You on request in a timely manner such information as is necessary to demonstrate compliance by Whatfix with its obligations under Data Protection Laws.
- Whatfix shall, upon reasonable notice, allow for and contribute to audits of Whatfix's Processing of Personal Data, as well as the TOMs (including data Processing systems, policies, procedures and records), during regular business hours and with minimal interruption to Whatfix's business operations. Such audits shall be conducted by You, Your affiliates or an independent third party on Your behalf (which will not be a competitor of Whatfix) that is subject to reasonable confidentiality obligations.
- You shall pay Whatfix reasonable costs of allowing or contributing to audits or inspections in accordance with clause 10.2 where You wish to conduct more than one audit or inspection every 12 months. Whatfix will immediately refer to You any requests received from national data protection authorities that relate to Whatfix's Processing of Personal Data unless explicitly prohibited.
- Whatfix undertakes to cooperate with You in its dealings with national data protection authorities and with any audit requests received from national data protection authorities.

10. Personal Data Breach Notification

- In respect of any Personal Data Breach (actual or reasonably suspected), Whatfix shall: notify You of a Personal Data Breach involving Whatfix or a subcontractor without undue delay and it shall be Your responsibility to inform the Supervisory Authority of such breach within 72 hours of notice by Whatfix;
- provide reasonable information, cooperation and assistance to You in relation to any action to be taken in response to a Personal Data Breach under Data Protection Laws, including regarding any communication of the Personal Data Breach to Data Subjects and national data protection authorities.

11. Subcontracting

- You consent to Whatfix engaging third party sub-processors as indicated in Appendix 1 to Process Personal Data to fulfil its obligations under the Agreement provided that, Whatfix will provide at least fifteen (15) days notice to Your account administrator prior to the appointment or replacement of any sub-processor. You may object to Whatfix's appointment or replacement of a sub-processor prior to its appointment or replacement, provided such objection is based on reasonable grounds relating to data protection. In such event, Whatfix will either not appoint or replace the sub-processor or, if this is not possible You may suspend or terminate the Service(s) (without prejudice to any fees incurred by You prior to such suspension or termination).

- Where Whatfix, with Your consent, subcontracts its obligations and rights under this DPA it shall do so only by way of a binding written contract with the sub-processor which imposes essentially the same obligations according to Art. 28 GDPR especially with regard to instructions and TOMs on the sub-processor as are imposed on Whatfix under this DPA.
- Where the sub-processor fails to fulfil its data protection obligations under the subcontracting agreement, Whatfix shall remain fully liable to You for the fulfilment of its obligations under this DPA and for the performance of the sub-processor's obligations.

12. International Data Transfers

- Whatfix shall at all times provide an adequate level of protection for the Personal Data, wherever processed, in accordance with the requirements of Data Protection Laws. Where Whatfix processes Personal Data under this Agreement that originates from the EEA (including United Kingdom) and/or Switzerland, any such processing shall be conditional on Whatfix complying with (and procuring any sub-processor comply with) the Model Clauses, which are incorporated by reference and form an integral part of this Agreement. Purely for the purposes of the descriptions in the Model Clauses and only as between Whatfix and You, Whatfix agrees that it is a "data importer" and Controller is the "data exporter" under the Model Clauses (notwithstanding that Controller is located outside the EEA). Further, Appendix 1 of this Agreement will take the place of Appendix 1 of the Model Clauses respectively.

13. Deletion or Return of Personal Data

- Upon termination or expiry of the Terms, upon request from the Customer, Whatfix shall delete all Customer Content, including Personal Data within 30 days of effective termination of Your account. Whatfix shall only retain the Customer Content, as is necessary for providing its Services for a period of 2 years from the date of termination or expiry of the Terms. Within such retention period, You may export the Customer Content by writing to Whatfix at privacy@whatfix.com. This requirement shall not apply to the extent that Whatfix is required by applicable law to retain some or all of the Personal Data, in which event Whatfix shall isolate and protect the Personal Data from any further processing except to the extent required by such law.

14. Your Obligations

- You shall: (i) have at all times during the term of this DPA appropriate technical and organisational measures to ensure a level of security appropriate to the risk to protect any Personal Data;
- provide clear and comprehensible written instructions to Whatfix for the Processing of Personal Data to be carried out under this DPA; and
- ensure that you have all the necessary licences, permissions, consents and notices in place to enable lawful transfer of Personal Data to Whatfix for the duration and purposes of this DPA.

15. Undertaking

- You acknowledge and agree that You are the Business and Whatfix the Service Provider with respect to any Personal Information of Consumers forming part of Customer Content. Whatfix will not sell, retain, use, or disclose Personal Information of Consumers that Whatfix processes on Your behalf when providing the SaaS Services under the Terms for any purpose other than for the specific purpose of providing the SaaS Services in accordance with the Terms and as part of the direct relationship between Whatfix and the Customer. Whatfix certifies that it understands the restrictions in this clause 15 and will comply with such restrictions.

16. Miscellaneous

- Whatfix may perform analytics on Customer Content to improve, enhance, support and operate the Service and compile statistical reports and record insights into usage patterns. You acknowledge that Whatfix uses Customer Content for the aforementioned purpose in compliance with applicable laws.
- In case of any conflict, the provisions of this DPA shall take precedence over the provisions of any other agreement with Whatfix.
- No party shall receive any remuneration for performing its obligations under this DPA except as explicitly set out herein or in another agreement.
- Where this DPA requires a "written notice" such notice can also be communicated per email to the other party. Notices shall be sent to the contact persons set out in Appendix 1.
- Any supplementary agreements or amendments to this DPA must be made in writing and signed by both parties.
- Should individual provisions of this DPA become void, invalid or non-viable, this shall not affect the validity of the remaining conditions of this Agreement.

The following Appendices form an integral part of this DPA:

APPENDIX 1

DETAILS OF THE PROCESSING OF PERSONAL DATA

- **Data subjects**

Data Subjects are those individuals whose Personal Data is transferred to the Processor pursuant to the Terms.

- **Categories of data**

Categories of data include Personal Data of the Users or the End-users of the Service(s) forming part of the Customer Content.

- **Processing operations**

Processor must process the data collected from or for the Controller or in connection with its services provided to the Controller solely to provide the services specified in the Service Agreement. The duration of processing will be as designated in the Service Agreement.

List of Sub-processors

SUB-PROCESSOR NAME	PURPOSE OF PROCESSING	TYPE OF DATA PROCESSED
AWS	For managing our cloud infrastructure (backup for DigitalOcean)	Name, Email id, Company Name, IP Address, Platform Activity Data
DigitalOcean	For managing our cloud infrastructure	Name, Email id, Company Name, IP Address, Platform Activity Data
Google Analytics	For better understanding our customers	IP Address and any other unique identifier mutually agreed between client and Whatfix

Azure	For managing our cloud infrastructure (backup for DigitalOcean)	Name, Email id, Company Name, IP Address, Platform Activity Data

APPENDIX 2

Standard Contractual Clauses

COMMISSION IMPLEMENTING DECISION (EU) 2021/914

of 4 June 2021

on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to 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 (General Data Protection Regulation) ([1]), and in particular Article 28(7) and Article 46(2)(c) thereof,

Whereas:

(1) Technological developments are facilitating cross-border data flows necessary for the expansion of international cooperation and international trade. At the same time, it is necessary to ensure that the level of protection of natural persons guaranteed by Regulation (EU) 2016/679 is not undermined where personal data is transferred to third countries, including in cases of onward transfers ([2]). The data transfer provisions in Chapter V of Regulation (EU) 2016/679 are intended to ensure the continuity of that high level of protection where personal data is transferred to a third country ([3]).

(2) Pursuant to Article 46(1) of Regulation (EU) 2016/679, in the absence of an adequacy decision by the Commission pursuant to Article 45(3), a controller or processor may transfer personal data to a third country only if it has provided appropriate safeguards, and on condition that enforceable rights and effective legal remedies for data subjects are available. Such safeguards may be provided for by standard data protection clauses adopted by the Commission pursuant to Article 46(2)(c).

(3) The role of standard contractual clauses is limited to ensuring appropriate data protection safeguards for international data transfers. Therefore, the controller or processor transferring the personal data to a third country (the 'data exporter') and the controller or processor receiving the personal data (the 'data importer') are free to include those standard contractual clauses in a wider contract and to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, the standard contractual clauses or prejudice the fundamental rights or freedoms of data subjects. Controllers and processors are encouraged to provide additional safeguards by means of contractual commitments that supplement the standard contractual clauses ([4]). The use of the standard contractual clauses is without prejudice to any contractual obligations of the data exporter and/or importer to ensure respect for applicable privileges and immunities.

(4) Beyond using standard contractual clauses to provide appropriate safeguards for transfers pursuant to Article 46(1) of Regulation (EU) 2016/679, the data exporter has to fulfil its general responsibilities as controller or processor under Regulation (EU) 2016/679. Those responsibilities include an obligation of the controller to provide data subjects with information about the fact that it intends to transfer their personal data to a third country pursuant to Article 13(1)(f) and Article 14(1)(f) of Regulation (EU) 2016/679. In the case of transfers pursuant to Article 46 of Regulation (EU) 2016/679, such information must include a reference to the appropriate safeguards and the means by which to obtain a copy of them or information where they have been made available.

([1]) OJ L 119, 4.5.2016, p. 1.

(2) Article 44 of Regulation (EU) 2016/679.
(3) See also judgment of the Court of Justice of 16 July 2020 in Case C-311/18, *Data Protection Commissioner* v *Facebook Ireland Ltd and Maximillian Schrems ('Schrems II')*, ECLI:EU:C:2020:559, paragraph 93.
(4) Recital 109 of Regulation (EU) 2016/679.

(5) Commission Decisions 2001/497/EC ([5]) and 2010/87/EU ([6]) contain standard contractual clauses to facilitate the transfer of personal data from a data controller established in the Union to a controller or processor established in a third country that does not offer an adequate level of protection. Those decisions were based on Directive 95/46/EC of the European Parliament and of the Council ([7]).

(6) Pursuant to Article 46(5) of Regulation (EU) 2016/679, Decision 2001/497/EC and Decision 2010/87/EU remain in force until amended, replaced or repealed, if necessary, by a Commission decision adopted pursuant to Article 46(2) of that Regulation. The standard contractual clauses in the decisions required updating in the light of new requirements in Regulation (EU) 2016/679. Moreover, since the decisions were adopted, the digital economy has seen significant developments, with the widespread use of new and more complex processing operations often involving multiple data importers and exporters, long and complex processing chains, and evolving business relationships. This calls for modernisation of the standard contractual clauses to reflect those realities better, by covering additional processing and transfer situations, and to allow a more flexible approach, for example with respect to the number of parties able to join the contract.

(7) A controller or processor may use the standard contractual clauses set out in the Annex to this Decision to provide appropriate safeguards within the meaning of Article 46(1) of Regulation (EU) 2016/679 for the transfer of personal data to a processor or controller established in a third country, without prejudice to the interpretation of the notion of international transfer in Regulation (EU) 2016/679. The standard contractual clauses may be used for such transfers only to the extent that the processing by the importer does not fall within the scope of Regulation (EU) 2016/679. This also includes the transfer of personal data by a controller or processor not established in the Union, to the extent that the processing is subject to Regulation (EU) 2016/679 (pursuant to Article 3(2) thereof), because it relates to the offering of goods or services to data subjects in the Union or the monitoring of their behaviour as far as it takes place within the Union.

(8) Given the general alignment of Regulation (EU) 2016/679 and Regulation (EU) 2018/1725 of the European Parliament and of the Council ([8]), it should be possible to use the standard contractual clauses also in the context of a contract, as referred to in Article 29(4) of Regulation (EU) 2018/1725 for the transfer of personal data to a sub- processor in a third country by a processor that is not a Union institution or body, but which is subject to Regulation (EU) 2016/679 and which processes personal data on behalf of a Union institution or body in accordance with Article 29 of Regulation (EU) 2018/1725. Provided the contract reflects the same data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) Regulation (EU) 2018/1725, in particular by providing sufficient guarantees for technical and organisational measures to ensure that the processing meets the requirements of that Regulation, this will ensure compliance with Article 29(4) of Regulation (EU) 2018/1725. In particular, that will be the case where the controller and processor use the standard contractual clauses in Commission Implementing Decision on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council ([9]).

(9) Where the processing involves data transfers from controllers subject to Regulation (EU) 2016/679 to processors outside its territorial scope or from processors subject to Regulation (EU) 2016/679 to sub-processors outside its territorial scope, the standard contractual clauses set out in the Annex to this Decision should also allow to fulfil the requirements of Article 28(3) and (4) of Regulation (EU) 2016/679.

(10) The standard contractual clauses set out in the Annex to this Decision combine general clauses with a modular approach to cater for various transfer scenarios and the complexity of modern processing chains. In addition to the general clauses, controllers and processors should select the module applicable to their situation, so as to tailor their obligations under the standard contractual clauses to their role and responsibilities in relation to the data processing

(5) Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC (OJ L 181, 4.7.2001, p. 19).

(6) Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (OJ L 39, 12.2.2010, p. 5).

(7) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with

regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

(8) 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); see recital 5.

(9) C(2021) 3701.

in question. It should be possible for more than two parties to adhere to the standard contractual clauses. Moreover, additional controllers and processors should be allowed to accede to the standard contractual clauses as data exporters or importers throughout the lifecycle of the contract of which they form a part.

(11) In order to provide appropriate safeguards, the standard contractual clauses should ensure that the personal data transferred on that basis is afforded a level of protection essentially equivalent to that guaranteed within the Union ([10]). With a view to ensuring transparency of processing, data subjects should be provided with a copy of the standard contractual clauses and be informed, in particular, of the categories of personal data processed, the right to obtain a copy of the standard contractual clauses, and any onward transfer. Onward transfers by the data importer to a third party in another third country should be allowed only if the third party accedes to the standard contractual clauses, if the continuity of protection is ensured otherwise, or in specific situations, such as on the basis of the explicit, informed consent of the data subject.

(12) With some exceptions, in particular as regards certain obligations that exclusively concern the relationship between the data exporter and data importer, data subjects should be able to invoke, and where necessary enforce, the standard contractual clauses as third-party beneficiaries. Therefore, while the parties should be allowed to choose the law of one of the Member States as governing the standard contractual clauses, that law must allow for third- party beneficiary rights. In order to facilitate individual redress, the standard contractual clauses should require the data importer to inform data subjects of a contact point and to deal promptly with any complaints or requests. In the event of a dispute between the data importer and a data subject who invokes his or her rights as a third-party beneficiary, the data subject should be able to lodge a complaint with the competent supervisory authority or refer the dispute to the competent courts in the EU.

(13) In order to ensure effective enforcement, the data importer should be required to submit to the jurisdiction of such authority and courts, and to commit to abide by any binding decision under the applicable Member State law. In particular, the data importer should agree to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. In addition, the data importer should have the option of offering data subjects the opportunity to seek redress before an independent dispute resolution body, at no cost. In line with Article 80(1) of Regulation (EU) 2016/679, data subjects should be allowed to be represented by associations or other bodies in disputes against the data importer if they so wish.

(14) The standard contractual clauses should provide for rules on liability between the parties and with respect to data subjects, and rules on indemnification between the parties. Where the data subject suffers material or non-material damage as a consequence of any breach of the third-party beneficiary rights under the standard contractual clauses, he or she should be entitled to compensation. This should be without prejudice to any liability under Regulation (EU) 2016/679.

(15) In the case of a transfer to a data importer acting as a processor or sub-processor, specific requirements should apply in accordance with Article 28(3) of Regulation (EU) 2016/679. The standard contractual clauses should require the data importer to make available all information necessary to demonstrate compliance with the obligations set out in the clauses and to allow for and contribute to audits of its processing activities by the data exporter. With respect to the engagement of any sub-processor by the data importer, in line with Article 28(2) and (4) of Regulation (EU) 2016/679, the standard contractual clauses should in particular set out the procedure for general or specific authorisation from the data exporter and the requirement for a written contract with the sub-processor ensuring the same level of protection as under the clauses.

(16) It is appropriate to provide different safeguards in the standard contractual clauses that cover the specific situation of a transfer of personal data by a processor in the Union to its controller in a third country and reflect the limited self- standing obligations for processors under Regulation (EU) 2016/679. In particular, the standard contractual clauses should require the processor to inform the controller if it is unable to follow its instructions, including if such instructions infringe Union data protection law, and require the controller to refrain from any actions that would prevent the processor from fulfilling its obligations under Regulation (EU) 2016/679. They should also require the parties to assist each other in responding to

enquiries and requests from data subjects under the local law applicable

([10]) *Schrems II*, paragraphs 96 and 103. See also Regulation (EU) 2016/679, recitals 108 and 114.

to the data importer or, for data processing in the Union, under Regulation (EU) 2016/679. Additional requirements to address any effects of the laws of the third country of destination on the controller's compliance with the clauses, in particular how to deal with binding requests from public authorities in the third country for disclosure of the transferred personal data, should apply where the Union processor combines the personal data received from the controller in the third country with personal data collected by the processor in the Union. Conversely, no such requirements are justified where the outsourcing merely involves the processing and transfer back of personal data that has been received from the controller and in any event has been and will remain subject to the jurisdiction of the third country in question.

(17) The parties should be able to demonstrate compliance with the standard contractual clauses. In particular, the data importer should be required to keep appropriate documentation for the processing activities under its responsibility and to inform the data exporter promptly if it is unable to comply with the clauses, for whatever reason. In turn, the data exporter should suspend the transfer and, in particularly serious cases, have the right to terminate the contract, insofar as it concerns the processing of personal data under standard contractual clauses, where the data importer is in breach of the clauses or unable to comply with them. Specific rules should apply where local laws affect compliance with the clauses. Personal data that has been transferred prior to the termination of the contract, and any copies thereof, should at the choice of the data exporter be returned to the data exporter or destroyed in their entirety.

(18) The standard contractual clauses should provide for specific safeguards, in particular in the light of the case law of the Court of Justice ([11]), to address any effects of the laws of the third country of destination on the data importer's compliance with the clauses, in particular how to deal with binding requests from public authorities in that country for disclosure of the transferred personal data.

(19) The transfer and processing of personal data under standard contractual clauses should not take place if the laws and practices of the third country of destination prevent the data importer from complying with the clauses. In this context, 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 should not be considered as being in conflict with the standard contractual clauses. The parties should warrant that, at the time of agreeing to the standard contractual clauses, they have no reason to believe that the laws and practices applicable to the data importer are not in line with these requirements.

(20) The parties should take account, in particular, of the specific circumstances of the transfer (such as the content and duration of the contract, the nature of the data to be transferred, the type of recipient, the purpose of the processing), the laws and practices of the third country of destination that are relevant in light of the circumstances of the transfer and any safeguards put in place to supplement those under the standard contractual clauses (including relevant contractual, technical and organisational measures applying to the transmission of personal data and its processing in the country of destination). As regards the impact of such laws and practices on compliance with the standard contractual clauses, different elements may be considered as part of an overall assessment, including reliable information on the application of the law in practice (such as case law and reports by independent oversight bodies), the existence or absence of requests in the same sector and, under strict conditions, the documented practical experience of the data exporter and/or data importer.

(21) The data importer should notify the data exporter if, after agreeing to the standard contractual clauses, it has reason to believe that it is not able to comply with the standard contractual clauses. If the data exporter receives such notification or otherwise becomes aware that the data importer is no longer able to comply with the standard contractual clauses, it should identify appropriate measures to address the situation, if necessary in consultation with the competent supervisory authority. Such measures may include supplementary measures adopted by the data exporter and/or data importer, such as technical or organisational measures to ensure security and confidentiality. The data exporter should be required to suspend the transfer if it considers that no appropriate safeguards can be ensured, or if so instructed by the

competent supervisory authority.

(11) *Schrems II*.

(22) Where possible, the data importer should notify the data exporter and the data subject if it receives a legally binding request from a public (including judicial) authority under the law of the country of destination for disclosure of personal data transferred pursuant to the standard contractual clauses. Similarly, it should notify them if it becomes aware of any direct access by public authorities to such personal data, in accordance with the law of the third country of destination. If, despite its best efforts, the data importer is not in a position to notify the data exporter and/or the data subject of specific disclosure requests, it should provide the data exporter with as much relevant information as possible on the requests. In addition, the data importer should provide the data exporter with aggregate information at regular intervals. The data importer should also be required to document any request for disclosure received and the response provided, and make that information available to the data exporter or the competent supervisory authority, or both, upon request. If, following a review of the legality of such a request under the laws of the country of destination, the data importer concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the third country of destination, it should challenge it, including, where appropriate, by exhausting available possibilities of appeal. In any event, if the data importer is no longer able to comply with the standard contractual clauses, it should inform the data exporter accordingly, including where this is the consequence of a request for disclosure.

(23) As stakeholder needs, technology and processing operations may change, the Commission should evaluate the operation of the standard contractual clauses in the light of experience, as part of the periodic evaluation of Regulation (EU) 2016/679 referred to in Article 97 of that Regulation.

(24) Decision 2001/497/EC and Decision 2010/87/EU should be repealed three months after the entry into force of this Decision. During that period, data exporters and data importers should, for the purpose of Article 46(1) of Regulation (EU) 2016/679, still be able to use the standard contractual clauses set out in Decisions 2001/497/EC and 2010/87/EU. For an additional period of 15 months, data exporters and data importers should, for the purpose of Article 46(1) of Regulation (EU) 2016/679, be able to continue to rely on standard contractual clauses set out in Decisions 2001/497/EC and 2010/87/EU for the performance of contracts concluded between them before the date of repeal of those decisions, provided that the processing operations that are the subject matter of the contract remain unchanged and that reliance on the clauses ensures that the transfer of personal data is subject to appropriate safeguards within the meaning of Article 46(1) of Regulation (EU) 2016/679. In the event of relevant changes to the contract, the data exporter should be required to rely on a new ground for data transfers under the contract, in particular by replacing the existing standard contractual clauses with the standard contractual clauses set out in the Annex to this Decision. The same should apply to any sub-contracting to a (sub-)processor of processing operations covered by the contract.

(25) The European Data Protection Supervisor and the European Data Protection Board were consulted in accordance with Article 42(1) and (2) of Regulation (EU) 2018/1725 and delivered a joint opinion on 14 January 2021 ([12]), which has been taken into consideration in the preparation of this Decision.

(26) The measures provided for in this Decision are in accordance with the opinion of the Committee established under Article 93 of Regulation (EU) 2016/679,

HAS ADOPTED THIS DECISION:

Article 1

1. The standard contractual clauses set out in the Annex are considered to provide appropriate safeguards within the meaning of Article 46(1) and (2)(c) of Regulation (EU) 2016/679 for the transfer by a controller or processor of personal data processed subject to that Regulation (data exporter) to a controller or (sub-)processor whose processing of the data is not subject to that Regulation (data importer).

2. The standard contractual clauses also set out the rights and obligations of controllers and processors with respect to the matters referred to in Article 28(3) and (4) of Regulation (EU) 2016/679, as regards the transfer of personal data from a controller to a processor, or from a processor to a sub-processor.

([12]) EDPB EDPS Joint Opinion 2/2021 on the European Commission's Implementing Decision on standard contractual clauses for the transfer of personal data to third countries for the matters referred to in Article 46(2)(c) of Regulation (EU) 2016/679.

Article 2

Where the competent Member State authorities exercise corrective powers pursuant to Article 58 of Regulation (EU) 2016/679 in response to the data importer being or becoming subject to laws or practices in the third country of destination that prevent it from complying with the standard contractual clauses set out in the Annex, leading to the suspension or ban of data transfers to third countries, the Member State concerned shall, without delay, inform the Commission, which will forward the information to the other Member States.

Article 3

The Commission shall evaluate the practical application of the standard contractual clauses set out in the Annex on the basis of all available information, as part of the periodic evaluation required by Article 97 of Regulation (EU) 2016/679.

Article 4

1. This Decision shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

2. Decision 2001/497/EC is repealed with effect from 27 September 2021.

3. Decision 2010/87/EU is repealed with effect from 27 September 2021.

4. Contracts concluded before 27 September 2021 on the basis of Decision 2001/497/EC or Decision 2010/87/EU shall be deemed to provide appropriate safeguards within the meaning of Article 46(1) of Regulation (EU) 2016/679 until 27 December 2022, provided the processing operations that are the subject matter of the contract remain unchanged and that reliance on those clauses ensures that the transfer of personal data is subject to appropriate safeguards.

Done at Brussels, 4 June 2021.

For the Commission The President

Ursula VON DER LEYEN

ANNEX

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;

(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.

(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

NOT USED

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 ONE: Transfer controller to controller

8.1 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. It may only process the personal data for another purpose:

(i) where it has obtained the data subject's prior consent;

(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

(iii) of the right to obtain a copy of these Clauses;

(iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties 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.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation ([2]) of the data and all back-ups at the end of the retention period.

8.5 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 personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (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.

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) 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 personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 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 or offences (hereinafter 'sensitive data'), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

(2) This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union ([3]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) it 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 with respect to the processing in question;

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

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

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

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

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and compliance

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

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.

(3) 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.

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 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 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.

(4) 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.

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 ([5]).

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).

(5) See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

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;

(6) 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 purposes of these Clauses.

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

(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.

MODULE FOUR: Transfer processor to controller

8.1 Instructions

(a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data

importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (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 of the personal data ([7]), the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

(c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) OPTION 1: SPECIFIC PRIOR AUTHORISATION The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least [*Specify time period*] prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

(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. ([8]) 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.

(7) This includes whether the transfer and further processing 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 or offences.

(8) This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

(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

(a) OPTION 1: SPECIFIC PRIOR AUTHORISATION The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the prior specific written authorisation of the controller. The data importer shall submit the request for specific authorisation at least [*Specify time period*] prior to the engagement of the sub-processor, together with the information necessary to enable the controller to decide on the authorisation. It shall inform the data exporter of such engagement. The list of sub- processors already authorised by the controller can be found in Annex III. The Parties shall keep Annex III up to date.

(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. ([9]) 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.

(9) This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

Clause 10

Data subject rights

MODULE ONE: Transfer controller to controller

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. ([10]) The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge:

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter 'automated decision'), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

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.

(10) That period may be extended by a maximum of two more months, to the extent necessary taking into account the

complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

(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.

MODULE FOUR: Transfer processor to controller

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

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 ONE: Transfer controller to controller

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.

(11) The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

(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 ONE: Transfer controller to controller 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 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 ONE: Transfer controller to

controller MODULE TWO: Transfer controller

to processor

MODULE THREE: Transfer processor 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 ONE:

Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to

processor

MODULE FOUR: Transfer processor to controller*(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)*

(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). [For Module Three: 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 [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.

Clause 15

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

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to

processor

MODULE FOUR: Transfer processor to controller *(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)*

(12) 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.

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.

For Module Three: 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.). For Module Three: 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. [For Module Three: 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

(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) [For Modules One, Two and Three: 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.] [For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] 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 ONE: Transfer controller to controller

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 England.

MODULE FOUR: Transfer processor to controller

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of England.

Clause 18

Choice of forum and jurisdiction

MODULE ONE: Transfer controller to controller

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 England.

(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.

MODULE FOUR: Transfer processor to controller

Any dispute arising from these Clauses shall be resolved by the courts of England.

ANNEX I

A. LIST OF PARTIES

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller

Controller(s): [Identity and contact details of the controller(s), and, where applicable, of the controller's data protection officer]

1. Name: _____
   Address: _____

2. _____

Contact person's name, position and contact details: _____

Processor(s): [Identity and contact details of the processor(s) and, where applicable, of the processor's data protection officer]

Name: QUICKO TECHNOSOFT LABS PVT LTD (**Parent company and its global subsidiaries**)
Address: 443, 17th Cross Road, Sector 4, HSR Layout, Bengaluru, Karnataka 560102

Contact person's name, position and contact details: SATYA MACHIRAJU,
DPO privacy@whatfix.com

B. DESCRIPTION OF TRANSFER

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller

Categories of data subjects whose personal data is processed

Data Subjects are those individuals whose Personal Data is transferred to the Processor pursuant to the terms of the Master Service Agreement.

Categories of personal data processed

Categories of data include Personal Data of the Users or the End-users of the Service(s) forming part of the Customer Content

Nature of the processing

- Processor must process the data collected from or for the Controller or in connection with its services
- provided to the Controller solely to provide the services specified in the Master Service Agreement.
- The duration of processing will be as designated in the Master Service Agreement

Purpose(s) for which the personal data is processed on behalf of the controller

To provide digital adoption services

Duration of the processing

During the Term of the Master Service Agreement

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

SUB-PROCESSOR NAME	PURPOSE OF PROCESSING	TYPE OF DATA PROCESSED
AWS, USA	For managing our cloud infrastructure (backup for DigitalOcean)	Name, Email id, Company Name, IP Address, Platform Activity Data
DigitalOcean, USA	For managing our cloud infrastructure	Name, Email id, Company Name, IP Address, Platform Activity Data
Azure	For managing our cloud infrastructure (backup for DigitalOcean)	Name, Email id, Company Name, IP Address, Platform Activity Data
Google Analytics, USA	For better understanding our customers	IP Address and any other unique identifier mutually agreed between client and Whatfix

C. COMPETENT SUPERVISORY AUTHORITY

MODULE ONE: Transfer controller to controller MODULE TWO: Transfer controller to processor MODULE THREE: Transfer processor to processor

ICO, UK

. . . . . .

ANNEX II

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

MODULE ONE: Transfer controller to controller MODULE TWO: Transfer controller to processor MODULE THREE: Transfer processor to processor

Whatfix maintains a formal information security program and information security team focused on protecting the information assets of our Customers.

The following provides a high-level overview of the measures Whatfix uses to provide a level of security appropriate to the risk of processing the Personal Data in connection with our services.

Category	Security Measures
Information security policies and framework, compliances	Whatfix is an ISO 27001:2013, CSA STAR certified organization and has SOC2 Type 2 Attestations. Whatfix maintains compliance to GDPR, CCPA and other applicable Regulations. Whatfix shall maintain and shall continue to maintain a written information security program that includes policies, procedures, and controls governing the Processing of Customer Content and data through Whatfix's solution (the "Information Security Program"). The Information Security Program is designed to protect the confidentiality, integrity, and availability of Customer Content by using a multi-tiered technical, procedural, and people-related control approach in accordance with industry best practices and applicable laws and regulations.
Physical and environmental security	Whatfix stores your data with the cloud platform of Amazon Web Services and Digital Ocean, which may store this data on their servers located outside of India. Amazon Web Services has security measures in place to protect the loss, misuse and alteration of the information, details of which are available at https://aws.amazon.com/. Digital Ocean has its security measures available at https://www.digitalocean.com/legal/data-security/. Whatfix shall maintain appropriate physical security measures designed to protect the tangible items, such as physical computer systems, networks, servers, and devices, that Process Customer Content. Whatfix shall utilize commercial grade security software and hardware to protect the Whatfix's service and the Production Environment. Whatfix shall ensure that: 1. Access to Whatfix's corporate facilities is tightly controlled; 2. All visitors to its corporate facilities sign in, agree to confidentiality obligations, and be escorted by Personnel while on premises at all times; and

	3. Visitor logs are reviewed by Whatfix's security team on a regular basis. 4. Personnel's physical access to Whatfix's corporate facilities upon termination of employment. 5. Its commercial-grade data center service providers used in the provision of Whatfix's solution maintain an on-site security operation that is responsible for all physical data center security functions and formal physical access procedures in accordance with SOC1 and SOC 2, or equivalent, standards. 6. The Data center provider has a SOC2 or equivalent certification/attestation for their scope of services to Whatfix.
Permitted Use of Customer Content	Whatfix will not access Customer Content in any manner except for what has been mutually agreed between Customer and Whatfix.
Acknowledgement of Shared Responsibilities	The security of data and information that is accessed, stored, shared, or otherwise Processed via a multi-tenant cloud service are shared responsibilities between a cloud service provider and Whatfix. As such, Whatfix is responsible for the implementation and operation of the Information Security Program and the protection measures described in the Agreement
Maintenance of Information Security Program	Whatfix shall take and implement appropriate technical and organizational measures to protect Customer Content located in Whatfix's system and shall maintain the Information Security Program in accordance with ISO 27001 standards or such other alternative standards that are substantially equivalent to ISO 27001. Whatfix shall update or modify the Information Security Program from time to time provided that such updates and modifications do not result in the degradation of the overall security of Whatfix's service.
Asset management	Whatfix maintains the assets in its cloud infrastructure, which are managed, and monitored by an internal cloud operations team. Our Asset management policies are in line with the controls of ISO 27001.
Human resource security	1. All employees working on the Whatfix Platform are subject to background verification and are bound by contractual obligations of confidentiality prior to being assigned to positions in which they will, or Whatfix reasonably expects them to, have access to Customer Content. 2. Employees go through various training sessions necessary to perform their duties, including training regarding information security. 3. Whatfix shall conduct a mandatory security awareness training to inform its Personnel on procedures and policies relevant to the Information Security Program and of the consequences of violating such procedures and policies.

Access Control Policy	Whatfix limits access to areas where customer data is processed and maintains audit logs of access and has implemented a strict role-based access control policy. Access Credentials Mechanism is as follows: All employees who have access to or maintain Controller data: ○ Have named access to the application/ infrastructure ○ Do not share user id/account with other users ○ Administrative Access to Systems is limited to only the cloud infrastructure (responsible for application upgrades and maintenance). ○ Portal administration access is limited to members from the Customer Success team associated with the Client Authorised personnel ○ Other employees DO NOT have access to Customer Content. User accounts are required to: ○ Have passwords expire at least every 90 days ○ Set to remember and not allow the use of at least the last 4 passwords ○ Where passwords are used, Processor requires the use of complex (upper/ lowercase alpha, special character, and a number) passwords. Whatfix shall maintain a formal access control policy and shall control Personnel access to the Production Environment. a) Whatfix shall maintain an associated access control process for reviewing and implementing Personnel access requests. b) Whatfix shall regularly review the access rights of authorized Personnel and, upon change in scope of employment necessitating removal or employment termination, remove or modify such access rights as appropriate. c) Whatfix shall monitor and assess the efficacy of access restrictions applicable to the control of Whatfix's system administrators in the Production Environment, which will entail generating system individual administrator activity information and retaining such information for a period of at least 12 months.
BCP and DR	● Whatfix has in place a documented Business Continuity / Disaster Recovery Plan, the Plan has been tested, reviewed, and updated annually. ● Regular Backups are performed and stored in a secure location and are encrypted. ● Whatfix shall maintain a written business continuity and disaster

	recovery plan that addresses the availability of Whatfix's solution ("Continuity Plan"). ● The Continuity Plan shall include elements such as: ○ crisis management plan and team activation, ○ event and communication process documentation; business recovery, ○ alternative site locations, ○ call tree testing; ○ and (c) infrastructure, ○ technology, system(s) details, ○ recovery activities, ○ and identification of the Personnel and teams required for such recovery. Whatfix shall, at a minimum, conduct a test of the Continuity Plan on an annual basis. Whatfix shall ensure that: ● infrastructure systems for Whatfix's solution have been designed to eliminate single points of failure and to minimize the impact of anticipated environmental risks; ● each data center supporting Whatfix's solution must include full redundancy and fault tolerance infrastructure for electrical, cooling, and network systems.
Security Incident communication management	● Whatfix will notify the customer in case of violation or breach of security resulting in a loss or unauthorized disclosure of customer data within 72 hours of breach identification. ● A formal information security incident management process is followed. ● Incidents are reported by an observer or internal teams monitoring activities and are acted upon immediately. ● The incident is contained first, to minimize impact, and then resolved. ● A root cause analysis is then performed and documented. Mitigation or resolution actions are performed and documented. Internal escalations are performed as needed. ● The entire incident is documented for generating a knowledge base.
Data Security and Privacy	● Whatfix treats data provided by Customer to the Platform as confidential.

	● Whatfix shall not use/process Customer personal information for any purposes other than listed in Whatfix Privacy Policy and/or Whatfix service agreement with the customer. ● Whatfix shall ensure that the personal data is not excessive for the stated legitimate business purposes in the Whatfix service agreement with the customer. ● Whatfix shall not share Customer's personal information with any third party other than listed in Whatfix Privacy Policy and/or Whatfix service agreement with the customer. ● Whatfix shall ensure the Customer data retention and disposition as per Whatfix Privacy policy and/or Whatfix service agreement with customer. Customer data must only be retained: ○ For as long as it is necessary to serve the relevant legitimate business purposes ○ To the extent necessary to comply with applicable law ○ To protect the right of data subject ● Whatfix shall implement technical and organizational measures to protect the customer data, including PII and has encrypted the customer data in transit and at rest. ● Whatfix shall ensure proper contractual safeguards (inline with GDPR) implemented in the event of personal data needs to be processed by, transferred by, gathered by or exchanged with any third party.
Risk Management	● Whatfix has identified and classified assets based on its criticality. ● Security risks related to the internal personnel, assets, and external parties (such as contractors, customers, and vendors) are identified and addressed via the ISO 27001: 2013 framework and applicable controls. ● Risk management is a continuous process adapted at Whatfix.
Personnel Policies and Procedures	● Whatfix has standard hiring and termination policies and procedures. ● The procedures include screening potential employees through an interview process, reference checks, formal offer letters, and new employee training. ● Employee disciplinary procedure and Human Resource Policy have been implemented. ● Upon hiring, employees are required to acknowledge that they understand the policies and procedures of the company by signing a 'Statement of Acceptance'. ● Whatfix also has developed a Non-Disclosure Agreement. Employees are required to sign the NonDisclosure Agreement, acknowledging that they will adhere to the company's policies and

	procedures. ● Policies relating to information security before hiring, during employment and on termination have been implemented as part of the Information Security Management System.
Network Security	● Whatfix shall maintain a defense-in-depth approach to hardening the Production Environment against exposure and attack. ● Whatfix shall maintain an isolated Production Environment that includes commercial grade network management controls such as load balancers, firewalls, intrusion detection systems distributed across production networks, and malware protections. ● Whatfix shall complement its Production Environment architecture with prevention and detection technologies that monitor all activity generated and send risk-based alerts to the relevant security groups.
Malicious Code Protection	Whatfix shall ensure that: ● its information systems and file transfer operations have effective and operational anti-virus software; ● all anti-virus software shall configured for deployment and automatic update; and ● applicable anti-virus software shall integrate with processes and shall automatically generate alerts to Whatfix's Cyber Incident Response Team if potentially harmful code is detected for their investigation and analysis.
Code Reviews	● Whatfix shall maintain a formal software development life cycle that includes secure coding practices against OWASP and related standards and shall perform both manual and automated code reviews. ● Whatfix's engineering, product development, and product operations management teams shall review changes included in production releases to verify that developers have performed automated and manual code reviews designed to minimize associated risks. ● In the event that a significant issue is identified in a code review, such issue shall be brought to Whatfix senior management's attention and shall be closely monitored until resolution prior to release into the Production Environment.
Vulnerability Scans and Penetration Tests	● Whatfix shall perform both internal and external vulnerability scanning and application scanning. ● External scans and penetration tests against Whatfix's solution and the Production Environment shall be conducted by both Internal teams as well as external qualified, credentialed, and industry recognized organizations.

	• Whatfix shall remedy vulnerabilities identified during scans and penetration tests in a commercially reasonable manner and timeframe based on severity. • Upon Customer's reasonable written request, Whatfix shall provide attestations resulting from vulnerability scans and penetration tests per independent external audit reports. • Upon prior notification, Customer is permitted to conduct any vulnerability scans or penetration testing against the Pre-Production Environment.
Separation	Whatfix shall separate Customer Content located in the Production Environment from other Whatfix customer data.
Encryption Technologies	• Whatfix shall encrypt Customer Content in accordance with industry best practice standards. • All access and transfer of data to and from Whatfix's solution shall be via HTTPS with minimum TLS 1.2 and Whatfix shall only support industry recognized and best practice cipher suites. • Whatfix shall encrypt all data persisted on the Production Environment with an AES 256-bit, or equivalent, encryption key.
Audit for Data Breach	• Whatfix shall use independent external auditors to verify the adequacy of its Information Security Program. • Upon Customer's reasonable written request, Whatfix will provide Customer with third party attestations, certifications, and reports relevant to the establishment, implementation, and control of the Information Security Program, including Whatfix's ISO 27001 certification and Service Organization Controls (SOC) reports. • Following a Data Breach, Whatfix shall, upon Customer's written request, promptly engage a third party independent auditor, selected by Whatfix and at Whatfix's expense, to conduct an on-site audit of Whatfix's Information Security Program, including Whatfix's data centers and corporate facilities relevant to the security of Customer Data. • Whatfix shall promptly provide the Customer with the report of such an audit.

ANNEX III

LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor MODULE THREE: Transfer processor to processor

EXPLANATORY NOTE:

This Annex must be completed for Modules Two and Three, in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

1. Name: **Amazon web services**
Address: 410 Terry Avenue North, Seattle, WA 98109-5210, USA
Address2: Amazon Web Services, Luxembourg
Contact person's name, position and contact details: https://aws.amazon.com/compliance/gdpr-center/
Description of the processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): As mentioned in the DPA

2. Name: **Digital Ocean**
Address: 101 6th Ave, New York, NY 10013, United States
Contact person's name, position and contact details: Alan Shapiro, General Counsel
Description of the processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): As mentioned in the DPA

3. Name: **Google LLC**
Address: 1600 Amphitheatre Parkway, Mountain View, California 94043 USA
Contact person's name, position and contact details:
https://support.google.com/policies/troubleshooter/9009584

4. Name: Azure, Microsoft
Address: Microsoft Ireland Operations Ltd. Attn: Privacy Officer Carmenhall Road Sandyford, Dublin 18, Ireland
Contact person's name, position and contact details: Customer may contact customer support or use Microsoft's Privacy web form, located at http://go.microsoft.com/?linkid=9846224