STANDARD CONTRACTUAL CLAUSES

Controller to Processor

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

The customer as defined in the Terms and Conditions located at https://www.Mandiant.com/company/legal or any separately negotiated agreement with Mandiant, Inc., as applicable, or the distributor, reseller or other partner as defined in the applicable agreement with Mandiant, Inc.

(the data exporter)

And

Name of the data importing organisation: Mandiant, Inc.

Address: 11951 Freedom Drive, 6th Floor, Reston, VA 20190

e-mail: Privacy@Mandiant.com

Other information needed to identify the organisation:

None.

(the data importer)

each a ‘party’; together ‘the parties’,

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

SECTION I

Clause 1

Purpose and scope

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

(b) The Parties:

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

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

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

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

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

Clause 2

Effect and invariability of the Clauses

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

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

Clause 3

Third-party beneficiaries

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

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

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

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

Clause 4

Interpretation

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

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

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7 – Optional

Docking clause

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

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

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

8.1 Instructions

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

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

8.2 Purpose limitation

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

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject

would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

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

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

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

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

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (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.

Clause 9

Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data

exporter with the information necessary to enable the data exporter to exercise its right to object.

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

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

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

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

Clause 10

Data subject rights

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

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

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

Clause 11

Redress

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

The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

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

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

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

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

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

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

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

Clause 12

Liability

(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

(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

(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;

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

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

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

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

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the 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

15.1 Notification

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

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

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

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

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

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

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

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

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

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

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

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

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

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

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

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii)

Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

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 Ireland.

Clause 18

Choice of forum and jurisdiction

(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 Ireland.

(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.

On behalf of the data importer: Mandiant, Inc.

Name: Richard Meamber

Position: General Counsel

Address: 11951 Freedom Drive, 6th Floor, Reston, VA 20190

Signature

Date: February 1, 2022


Mandiant, Inc.
CORPORATE
SEAL
February 18,
2004
DELAWARE

ANNEX I

A. LIST OF PARTIES

Data exporter:

The customer as defined in the Terms and Conditions located at https://www.Mandiant.com/company/legal.html or any separately negotiated agreement with Mandiant, Inc., as applicable, or the distributor, reseller or other partner as defined in the applicable agreement with Mandiant, Inc.

Role (controller/processor): Controller

Data importer(s):

Name: Mandiant, Inc.

Address: 11951 Freedom Drive, 6th Floor, Reston, VA 20190

Contact person's name, position and contact details: Richard Weaver, Data Protection Officer, Privacy@Mandiant.com; Ruth Kelleher, EU Representative, Privacy@Mandiant.com

Activities relevant to the data transferred under these Clauses:

Cybersecurity services.

Signature and date: 

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:

Users of the data exporter's network, endpoints, or other devices or systems.

Categories of personal data transferred:

Information collected (a) during security investigations, investigations into possible security breaches, and/or evaluations of data exporter's security practices; and (b) by security products, including security alerts generated by data importer's endpoint, network and email products.

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

Depending on the circumstances of the engagement, the personal data transferred to the data importer may include any, or all, types of special category personal data.

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

Continuous

Purpose(s) of the data transfer and further processing

Cybersecurity services.

C. COMPETENT SUPERVISORY AUTHORITY

Ireland

…

ANNEX II

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

Mandiant maintains a formal Program designed to protect Mandiant's information processing systems from internal and external security threats, loss, and unauthorized disclosure. Mandiant has an internal Information Security Policy Framework, and Information Security Policies within that Framework, that are approved by Mandiant's management and is published and communicated to Mandiant personnel. The Information Security Policies comply with applicable local, state and federal laws, are designed based on guidance from ISO/IEC 27001:2013 and NIST 800-53 rev4 and shall align with all applicable industry-standards and best practices including but not limited to the American Institute of Certified Public Accountants ("AICPA"), Service Organization Controls ("SOC2"), PCI-DSS, CIS, FedRAMP, UK Cyber Essentials, TISAX, and CREST.

The Mandiant Information Security Policies are reviewed and updated periodically in the event of significant changes to applicable law, Mandiant architecture, or available technologies. Mandiant addresses breaches of security policies and procedures, including interfering with or otherwise compromising security measures, through a formal disciplinary process.

1. **Information Assets**: Mandiant has documented policies and procedures regarding the acceptable use of information, electronic and computing devices, and network resources to conduct Mandiant business or interact with internal networks and business systems, whether owned or leased by Mandiant, Mandiant personnel, or a third party. These policies and procedures also specify that all computer equipment, networking infrastructure, software, operating systems, storage media, smartphones supplied by Mandiant and network accounts are the property of Mandiant/FireEye. These systems are to be used for business purposes in serving the interests of the company and our customers in the course of normal operations. All Mandiant personnel, contractors, and other workers at Mandiant and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Mandiant policies and standards, and local laws and regulation.
2. **Data Retention:** Mandiant has established policies and procedures regarding the retention of client data based on its type and sensitivity. Once client data retention periods expire, automated scripts are used to remove data from Mandiant production systems. Mandiant destruction methods are consistent with industry guidelines such as NIST 800-88.
3. **Risk Assessment**: Periodic risk assessments are performed on critical information systems, networks and applications. These assessments identify relevant risks and threats to the organization, estimates the significance of the identified risks and impact, assesses the likelihood of their occurrence and decides on remediation and/or mitigation actions. Mandiant also has a Risk Management Charter that establishes the minimum requirements

and procedural steps for a Risk Exception. Such exceptions are temporary deviations from the organizational policies, procedures, standards and/or guidelines, and must addressed as specified by the cognizant review authorities.

4. **Access Controls**: Mandiant implemented robust access controls based on "least privilege" throughout our system architecture. Account entitlement and privilege are designed based on the level of access needed to perform job function. Administrative accounts or accounts with administrative privilege are only used for administrative activity and only for the time that such activity is necessary. Use of administrator privileges is appropriately logged within the system as evidence of the work performed. Some IT roles (such as a network admin) may possess multiple accounts, logging in as a standard user for routine tasks, while logging into a privileged account to perform administrative activities. Mandiant requires User IDs and strong authentication (which may include password requirements and/or tokens) to access Customer Information located on Mandiant systems.
5. **Security Controls**: Mandiant implements controls to mitigate information security risks. Controls may be physical, technical or administrative in their operation, and they may be preventative, detective, corrective, deterrent or recovery-focused in their intent. Controls may include hardware and software functions, processes and procedures, organizational and managerial structures. Controls are reviewed periodically to ensure they are still appropriate.
6. **Logical Security**: Mandiant implements logical security in relation to the services performed for customer, designed to:
    - Prevent unauthorized individuals from gaining access to customer systems; and
    - Reduce the risk of misuse of customer systems or Customer Information; and
    - Detect any security breaches that do occur enabling quick rectification of any problems that result and identification of the individuals who obtained access and determination.
7. **Physical Security**: Mandiant's data centers and the collocated data center(s) used by Mandiant are equipped with strong physical security controls and certified to comply with industry-accepted security standards, such as SOC 2, ISO27001, and PCI DSS standard. Globally, Mandiant data centers and facilities are protected with physical security controls that include:
    - Electronic controlled access system (badge reader, biometric reader, etc.)
    - Cipher locks (electronic or mechanical) to control access within or to the facility
    - Security guards that provide onsite security services
    - Entry and exit doors alarmed and monitored by security guards
    - External lighting
    - Lighting on all doors
    - Exterior doors with external hinge pins
    - Windows with contact or break alarms on all windows

    The Mandiant owned system assets and data reside in a designated area in the data center and protected by Mandiant owned access control system, in addition to the physical security controls provided by the data center provider. Activities are monitored by Mandiant Global Security Operational Center 24x7. Access to the Mandiant data center area must be

authorized and adhere to our data center access management procedures. A visitor with approval must be escorted at all time during the visit.

8. **Data Security:** All data transited by a Mandiant product is encrypted by default. Other data in transit (that is not associated with a Mandiant product) is encrypted using either our Accellion Kiteworks secure transfer service (which is FIPS 140-2 compliant), or the client's secure file transfer services. Mandiant has controls in place to protect data at rest.

9. **Security Monitoring**: The Mandiant Information Security & Risk Management team (InfoSec) has its own internal and independent Security Operation Center (SOC), which is separate from the Mandiant hosted product and services teams. The InfoSec SOC members review the logs and track, identify, and investigate the anomalies on a routine and continuous basis. Mandiant protects logging facilities and log information against tampering and unauthorized access.

   Mandiant has a standard network security stack deployed at each corporate location consisting of FireEye Network Security NX (advanced network threat protection), FireEye Network Forensics PX (full packet capture), and FireEye Helix Cloud Collector (IDS, network situational awareness).

   Each Mandiant workstation has FireEye Endpoint Security HX installed as the Enterprise Detection and Response (EDR) capability. Mandiant email is protected against advanced threats using FireEye's Email Security ETP product. Finally, Mandiant monitors cloud environments using FireEye's Helix product performing analytics against AWS CloudTrail logs and other log sources. Mandiant treats wireless networks the same as wired networks and uses Wi-Fi Protected Access II (WPA2) to secure wireless networks. Mandiant requires Mandiant employees to VPN into corporate data centers from wireless networks.

10. **Vulnerability Management**: Mandiant conducts regular automated vulnerability scans of the Mandiant environment and systems using commercially available tools and third-party penetration testing partners. Identified vulnerabilities are reviewed, triaged and remediated per the defined remediation SLA requirement. Mandiant applies, tests, and validates Mandiant application patches and updates before distribution.

11. **Vendor Assessment**: Mandiant has a formal enterprise Vendor Assessment Program, led by the Mandiant Information Security (InfoSec) Governance, Risk, and Compliance (GRC) Team, for evaluating the cybersecurity and data protection practices of Mandiant's third-party vendors and service providers to ensure they meet Mandiant's requirements for information security and data privacy as well as industry standards and applicable laws and regulations (e.g., data protection regulation).

    A Vendor Risk Assessment must be completed when Mandiant (a) engages a new vendor or new product/service, (b) engages a new product/service from an existing vendor, and (3) renews an existing vendor for specific products/services. The level of vendor risk assessment required varies depending on the nature of the vendor's service and how Mandiant involves the vendor.

Typically, the vendor risk assessment is conducted via a pre-built questionnaire that contains a series of questions to assess the vendor's information security and data privacy practices. The provided answers and supporting documentation are reviewed by InfoSec GRC, the Security Architecture Team, and the Mandiant Data Protection Officer, as needed, for assessing the vendor's risk. Vendors that do not meet Mandiant's InfoSec requirements are unable to continue business with Mandiant/FireEye.

InfoSec also works with the Privacy and Legal Teams to ensure that necessary confidentiality, information security, and data protection terms are incorporated in the vendor contract. Once approved, the Mandiant InfoSec GRC Team monitors its third-party vendors for compliance against the contracted security language and requisite technical obligations.

12. **Incident Response**: Mandiant has a Security Incident Management Program and formal Incident Response (IR) Plan encompassing response procedures for information security or privacy event. The IR Plan outlines:
    - Roles and responsibilities of the IR Team, available 24x7x365.
    - Procedures to respond to a reported incident based on the type of incident and severity.
    - Procedures to maintain chain-of-custody for evidence during incident investigations.
    - Reporting requirements and mechanisms to support the necessary communications.
    - Process for client and third-party notifications (e.g., legal, regulatory, and contractual).
    - Formal disciplinary process for dealing with those who commit a security violation.
    - Root cause analysis and remediation plan following incident.
13. **Software Development Lifecycle:** Mandiant uses a formal software development lifecycle process. Mandiant incorporates software and application security throughout its product development organization and processes. The focus of these initiatives is to "build security in" to Mandiant products and prevent security issues from being introduced. Mandiant's product security initiatives are based on industry maturity models and include a dedicated Product Security Group, a Security Champion on each development team, a secure development training program, use of a variety of application security tools, automated and manual code reviews, and security vulnerability assessment and penetration testing of Mandiant products.
14. **Business Continuity and Disaster Recovery (BC/DR)**: In addition to standard processes and procedures for the backup and recovery of data, Mandiant tests its Business Continuity (BC) and Disaster Recovery (DR) plans at least annually. These exercises and tests include evacuation drills, hybrid table-top exercises, and functional testing where possible and necessary. Mandiant tests specific business activities and scenarios of specific resources, including people, technology and facilities become unavailable under disruptive event. Mandiant also tests scenarios whereby its information and communication technologies and networks are impacted by dedicated cyber-attacks. The results are documented, evaluated, and scheduled for remediation within the next review cycle.

15. **Background Checks**: Background verification for employment candidates is a mandatory component of Mandiant's hiring process. All personnel are required to sign a confidentiality and non-disclosure agreement agreeing not to disclose proprietary or confidential information including client information to unauthorized parties. In accordance with applicable law, Mandiant's employee background checks traditionally consist of the following:

    - Verification of identity.
    - Criminal check.
    - Global sanctions check.
    - Verification of the information provided on the third-party application, including employment experience and educational credentials.
    - Depending on the circumstances, checks may also include credit history checks, drug screening, and social media reviews.

16. **Cybersecurity Training**: Mandiant personnel are trained and notified of information security requirements and employee responsibilities. Mandiant personnel with responsibility for the development and implementation of information security systems are qualified and capable of performing required security-related functions. The Mandiant Security Awareness training program is in place to maintain the skill level of personnel regarding security and privacy expectations and best practices.

ANNEX III

LIST OF SUB-PROCESSORS

The controller has authorised the use of the sub-processors listed on the processor's customer support portal under a general authorisation and the following sub-processors under a specific authorisation:

1. Name: Amazon Web Services (AWS)
   Address: 440 Terry Ave N., Seattle, WA 98109
   Contact person's name and contact details can be found here:
   https://aws.amazon.com/privacy/
   Description of processing: cloud hosting and storage

2. Name: Atlassian
   Address: 350 Bush Street Floor 13, San Francisco, CA 94104
   Contact person's name and contact details can be found here:
   https://www.atlassian.com/legal/privacy-policy
   Description of processing: customer ticketing and project management

3. Name: Azure
   Address: 1 Microsoft Way, Redmond, WA 98052
   Contact person's name and contact details can be found here:
   https://privacy.microsoft.com/en-us/privacystatement
   Description of processing: cloud hosting and storage

4. Name: Digital Ocean, LLC
   Address: 101 Avenue of the Americas, New York, NY 10013
   Contact person's name and contact details can be found here:
   https://www.digitalocean.com/legal/privacy-policy/
   Description of processing: Red Teaming

5. Name: FireEye Security Holdings US LLC
   Address: 6000 Headquarters Drive, Suite 600, Plano TX 75024
   Contract person's name and contact details can be found here:
   https://www.fireeye.com/company/privacy.html
   Description of processing: cybersecurity services

6. Name: Google LLC
   Address: 1600 Amphitheatre Parkway, Mountain View, CA 94043
   Contact person's name and contact details can be found here:
   https://policies.google.com/privacy
   Description of processing: translation services and Mandiant Advantage

7. Hatching International B.V.
   Hermitage 138
   1506 TX
   Zaandam
   The Netherlands
   Contact person's name and contact details can be found here: https://hatching.io/about/#
   Description of processing: File/malware analysis

8. Name: Okta
   Address: 100 First Street, 6th Floor, San Francisco, CA 94105
   Contact person's name and contact details can be found here:
   https://www.okta.com/privacy-policy/
   Description of processing: Identity Authentication Management

9. Salesforce.com, Inc.
   Address: 415 Mission St., 3rd Floor, San Francisco, CA 94105
   Contact person's name and contact details can be found here:
   https://www.salesforce.com/company/privacy/
   Description of processing: customer ticketing

10. Snowflake, Inc.
    106 East Babcock Street, Suite 3A
    Bozeman, Montana 59715
    Contact person's name and contact details can be found here:
    https://www.snowflake.com/privacy-policy/
    Description of processing: Mandiant Advantage

11. VMRay, Inc.
    22 Boston Wharf Road, 7th Floor
    Boston, MA 02210
    Contact person's name and contact details can be found here:
    https://www.vmray.com/privacy-policy/
    Description of processing: File/malware analysis