FME Cloud Data Processing Addendum

INSTRUCTIONS:

1. Please complete pages 7 & 23, and then sign on page 7.
2. Send the completed and signed DPA to privacy@safe.com.
3. We will countersign and send you a final copy. We will reach out to you if there are any issues.

Last Modified: December 9, 2022

FME Cloud Data Processing Addendum

Safe Software Inc. ("Safe Software") and the counterparty agreeing to these terms ("Customer") have entered into an agreement available at https://www.safe.com/terms-and-conditions/fme-cloud-terms-of-use/ (the "Terms"), for the provision of FME Cloud online services (the "Online Services") and related technical support. This FME Cloud Data Processing Addendum and its Attachments (the "DPA") is entered into by Safe Software and Customer and supplements the Terms. In the event of a conflict between any parts of the Terms, then this DPA shall prevail.

1. Definitions

1.1. In this DPA:

"*Controller*" means the entity, by itself or jointly with another Controller, which determines the purposes and means of the Processing of Personal Data. The Controller means the "*Business*" under the CCPA.

"*Customer Data*" means the data, including Personal Data, that is processed by Safe Software on behalf of the Customer.

"*Data Incident*" means a breach of Safe Software's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data, including Personal Data, on systems managed or controlled by Safe Software.

"*Data Protection Laws*" means all laws, regulations and court orders which apply to the processing of Personal Data, including (i) Canada's Personal Information Protection & Electronic Documents Act ("PIPEDA"); (ii) European Union Regulation (EU) 2016/679 (General Data Protection Regulation) ("GDPR"); (iii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector ("ePrivacy Directive"); (iv) GDPR as it forms parts of the United Kingdom domestic law by virtue of Section 3 of the European Union (Withdrawal) Act 2018 ("UK GDPR"); and (iv) Swiss Federal Data Protection Act on 19 June 1992 and its Ordinance ("Swiss DPA"); and (iii) California Consumer Privacy Act of 2018 (CCPA)/California Privacy Rights Act of 2020 (CPRA), each as amended from time to time.

"*Data Subject*" means a natural person residing in the European Union, or any other country that has substantially adopted the GDPR provisions as part of their Data Protection Laws, whose Personal Data is subject to Processing by a Controller or Processor.

"*Personal Data*" means any information related to a Data Subject that can be used to directly or indirectly identify such Data Subject.

"*Processing*" means any operation or set of operations which is performed on Personal Data whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"*Processor*" means the entity which processes Personal Data on behalf of the Controller. The Processor means the "*Service Provider*" under the CCPA.

"SCCs" means the Standard Contractual Clauses annexed to the European Commission's Decision (EU) 2021/914 of 4 June 2021 as may be amended, superseded or replaced.

"*Sub-Processor*" means any Processor engaged by Safe Software to process Customer Data on its behalf.

"UK Addendum" means the International Data Transfer Addendum issued by the UK Information Commissioner under section 119A(1) of the Data Protection Act 2018 as may be amended, superseded, or replaced.

2. Details of the Processing

See Annex I of the Appendix to the SCCs (attached).

3. Obligations of the Parties

3.1. Role of the Parties. Unless section 3.4 applies, the parties acknowledge and agree that with regard to the Processing of Customer Data via the Online Services, Customer is the Controller and Safe Software is the Processor. This DPA does not apply where Safe Software processes Personal Data as a Controller, for example where Safe Software processes Customer's authentication credentials and payment information used to provision Customer's access to the Online Services.

3.2. Customer's Processing of Personal Data. Customer shall, in its use of the Online Services, conduct all Processing of Personal Data in accordance with the requirements of Data Protection Laws. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data and obtained consent for the Processing of Personal Data as contemplated in the Terms.

3.3. Safe Software's Processing of Personal Data. Safe Software shall conduct all Processing of Personal Data in accordance with the requirements of Data Protection Laws and in accordance with Customer's documented reasonable instructions.

3.4. Authorization by Third Party Controller. If Customer is a Processor for a third party Controller, Customer warrants to Safe Software that Customer's instructions and actions with respect to Customer Data, including its appointment of Safe Software as another Processor, have been authorized by the third party Controller.

3.5. MSP Partner as Controller. If Customer has directly contracted with one of Safe Software's MSP Partners to provide services or support related to the Online Services, then Customer expressly agrees that such MSP Partner is considered to be a Controller and not a Sub-Processor under this DPA.

4. Rights of Data Subjects

4.1. Corrections & Deletions. The Customer is responsible for safeguarding the rights of Data Subjects. To the extent Customer, in its use of the Online Services, does not have the ability to correct, amend, block or delete Personal Data, as required by Data Protection Laws, Safe Software shall comply with any commercially reasonable written request by Customer to facilitate such actions to the extent Safe Software is legally permitted to do so.

4.2. Data Subject Requests. Safe Software shall promptly notify Customer if it receives a request from a Data Subject to exercise its rights under any Data Protection Laws and will refer such request to the Customer. Safe Software shall not respond to any such Data Subject's request except to confirm that such request relates to Customer. Safe Software shall provide Customer with commercially reasonable cooperation and assistance in relation to handling of a Data Subject's request for that person's Personal Data, to the extent legally permitted and to the extent Customer does not have access to such Personal Data through its use or receipt of the Online Services.

5. Security

5.1. Controls for the Protection of Personal Data. Taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Safe Software shall implement and maintain appropriate technical and organizational measures to protect Personal Data against accidental or unlawful destruction, loss, damage, theft, alteration, unauthorized disclosure or access.

5.2. Safe Software Personnel. Safe Software shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities, and are under appropriate statutory or contractual obligations of confidentiality. Safe Software shall ensure that Safe Software's access to Personal Data is limited to those personnel who require such access to perform the Online Services and related technical support.

5.3. Third-Party Certifications and Audits. Safe Software has obtained third party security audits. Upon Customer's written request at reasonable intervals, and subject to reasonable confidentiality obligations, Safe Software shall make available to Customer a summary or copy of Safe Software's most recent third-party audits, as applicable.

5.4. Customer's Security Responsibilities. Customer agrees that it is solely responsible for its use of the Online Services including making appropriate use of the Online Services to ensure a level of security appropriate to the risk in respect of Customer Data, applying security patches provided by Safe Software, and securing the authentication credentials, ports, systems and devices Customer uses to access the Online Services. For more information on Customer's responsibilities please see the FME Cloud Shared Responsibility Model which is located here: https://www.safe.com/terms-and-conditions/fme-cloud-support-policy/#shared-responsibility.

6. Data Incidents

6.1. Incident Notification. Safe Software maintains data incident management policies and procedures and shall, to the extent required by law, notify Customer without undue delay of any Data Incident and provide details of such Data Incident to the Customer. To the extent such Data Incident is caused by a violation of the requirements of this DPA by Safe Software, Safe Software shall promptly take reasonable steps to minimize harm and identify and remediate the cause of such Data Incident.

6.2. Delivery of Notification. Safe Software will deliver notification of any Data Incident that requires reporting to the emergency contact supplied by Customer at the time of provisioning the Online Services, or as updated by the Customer from time to time. Customer is solely responsible for providing the emergency contact information and ensuring it is updated. Safe Software, in its sole discretion (including if Customer has not provided an emergency contact), may elect to provide notification by any other reasonable means of communication.

6.3. Third Party Notifications. Customer is solely responsible for complying with incident notification laws or requirements applicable to Customer and fulfilling any third party notification obligations related to any Data Incident.

6.4. No acknowledgment of Fault. Safe Software's notification or response to any Data Incident will not be construed as an acknowledgment by Safe Software of any fault or liability with respect to the Data Incident.

7. Deletion of Customer Data

To the extent permitted by law, upon termination of Customer's use of the Online Services, Safe Software will promptly delete Customer Data in accordance with Safe Software's procedures.

8. Transfer of Data

8.1 International Data Transfer. As part of procuring the Online Services, Customer will elect a region where the primary Processing of Customer Data will occur. However, Customer agrees that Safe Software may process Customer Data in Canada and the USA as required from time to time to provide the Online Services and related technical support. Whenever Personal Data is transferred outside its country of origin, each party will ensure such transfers are made in compliance with the requirements of Data Protection Laws.

8.2 Compliance. Safe Software will not transfer Personal Data to any country or recipient not recognized as providing an adequate level of protection for Personal Data (within the meaning of the GDPR and other applicable Data Protections Laws), unless it first takes all such measures as are necessary to ensure the transfer is in compliance with applicable Data Protection Laws. Such measures may include (without limitation) transferring such data to a recipient that is covered by a suitable framework or other legally adequate transfer mechanism recognized by the relevant authorities or courts as providing an adequate level of protection for Personal Data, to a recipient that has achieved binding corporate rules authorization in accordance with Data Protection Laws, or to a recipient that has executed appropriate standard contractual clauses in each case as adopted or approved in accordance with applicable Data Protection Laws.

8.3 Transfer Mechanism. Customer acknowledges that in connection with the performance of the Online Services, Safe Software is a recipient of Personal Data in Canada, which is deemed to be an adequate country under Data Protection Laws. Customer also acknowledges that Safe Software engages Sub-Processors that may be based in the United States. The parties agree that the SCCs (attached as Attachment 1 to this DPA) and the UK Addendum (attached as Attachment 2 to this DPA) will be incorporated by reference and form part of the DPA as follows:

(a) *EEA Transfers*. In relation to Personal Data of that is subject to the GDPR: (i) the Customer is the "data exporter" and Safe Software is the "data importer"; (ii) the Module Two terms of the SCC apply to the extent the Customer is the Controller and the Module Three terms of the SCC apply to the extent that Customer is a Processor; (iii) in Clause 7, the optional docking clause does apply; (iv) in Clause 9, Option 2 applies and changes to Sub-Processors will be notified in accordance with '*Section 9. Sub-Processors'* of this DPA; (v) in Clause 11, the optional language is deleted; (vi) in Clauses 17 and 18, the parties agree that the governing law and forum for disputes for the SCCs will be the Republic of Ireland; and (vii) if and to the extent the SCCs conflict with any provision of this DPA the SCCs will prevail to the extent of such conflict.

(b) *UK Transfers*. In relation to Personal Data that is subject to the UK GDPR, the SCCs will apply in accordance with sub-section (a) and the following modifications: (i) the SCCs will be modified and interpreted in accordance with the UK Addendum, which will be incorporated by reference and form an integral part of the Agreement; (ii) Tables 1, 2 and 3 of the UK Addendum will be deemed completed with the information set out in the Annexes of this SCCs and Table 4 will be deemed completed by selecting "neither party"; and (iii) any conflict between the terms of the SCCs and the UK Addendum will be resolved in accordance with Section 10 and Section 11 of the UK Addendum.

(c) *Swiss Transfers*. In relation to Personal Data that is subject to the Swiss DPA, the SCCs will apply in accordance with sub section (a) and the following modifications (i) references to "Regulation (EU) 2016/679" will be interpreted as references to the Swiss DPA; (ii) references to "EU", "Union" and "Member State law" will be interpreted as references to Swiss law; and (iii) references to the "competent supervisory authority" and "competent courts" will be replaced with the "the Swiss Federal Data Protection and Information Commissioner " and the "relevant courts in Switzerland".

8.4 Non-Compliance. If Safe Software cannot comply with its obligations under the SCCs or is in breach of any warranties under the SCCs or UK Addendum (as applicable) for any reason, and you intend to suspend the transfer of Personal Data to Safe Software or terminate the SCCs, or UK Addendum, you agree to provide us with reasonable notice to enable us to cure such noncompliance and reasonably cooperate with us to identify what additional safeguards, if any, may be implemented to remedy such noncompliance. If we have not or cannot cure the non-compliance, you may terminate the Online Services in accordance with the Terms without liability to either party other than Safe Software will provide you with a prorated refund of all prepaid amounts for the period after such termination date.

9. Sub-Processors

9.1. Appointment of Sub-Processors. Customer acknowledges and agrees that Safe Software may engage third party Sub-Processors in connection with the provision of the Online Services and hereby consents to the use of all current Sub-Processors. A list of current Sub-Processors is available on our GDPR page located here: https://www.safe.com/legal/gdpr/.

9.2. Objection to Intended Sub-Processors. The list of Sub-Processors at https://www.safe.com/legal/gdpr/ will be updated as changes occur. To subscribe to advance notification of any such updates please contact privacy@safe.com. Customer may object to such updates within 14 days from receiving an email notification or from the date that any updates were made to https://www.safe.com/legal/gdpr/, whichever is later. If the Customer objects to the proposed Sub-Processor and Safe Software cannot reasonably accommodate Customer's objection, then Safe Software will notify Customer and provide the Customer with the option to terminate the Online Services and receive a prorated refund of all prepaid amounts for the period after such termination date.

9.3. Agreement with Sub-Processors. Safe Software has entered into a written agreement with each Sub-Processor containing data protection obligations not less protective than those in this DPA, to the extent applicable to the nature of the services provided by such Sub-Processor.

9.4. Liability. Safe Software shall be liable for the acts and omissions of its Sub-Processors to the same extent Safe Software would be liable if performing the services of each Sub-Processor directly under the terms of this DPA, except as otherwise set forth in the Terms.

10. Assistance

10.1. Cooperation and Assistance. Safe Software shall provide reasonable assistance, information, and cooperation to the Customer to ensure compliance with the Customer's obligations under Data Protection Laws. All reasonable expenses incurred by Safe Software resulting from this subsection will be reimbursed by Customer, provided that Safe Software notifies Customer in advance of such expenses.

10.2. Demonstrating Compliance. Safe Software shall make available to the Customer all information reasonably necessary to demonstrate compliance with Safe Software's obligations under this DPA. Further, Safe Software will allow for and contribute to audits or inspections conducted by the Customer, or a third party auditor appointed by Customer, to verify Safe Software's compliance with its obligations under this DPA. Audits shall be conducted at a mutually agreeable dates and times and in such a manner as not to unreasonably interfere with Safe Software's normal business activities. Safe Software may require that the persons conducting the audit sign confidentiality agreements, comply with Safe Software's applicable policies with respect to privacy and security, and comply with Data Protection Laws. Customer shall bear the cost for such audits unless Safe Software is shown to be in material noncompliance.

11. General Provisions

11.1 Severability. If any individual provisions of this DPA are determined to be invalid or unenforceable, the validity and enforceability of the other provisions of this DPA will not be affected.

11.2 Governing Law. This DPA will be governed, construed, interpreted, and enforced in accordance with the laws of the Province of British Columbia and the laws of Canada, unless otherwise required by the Data Protection Laws.

[signatures on next page]

The parties' authorized signatories have duly executed this DPA:

SAFE SOFTWARE INC.

Signature: _____

Name: _____

Title: _____

Date: _____

CUSTOMER

Entity Legal Name: _____

Signature:_____

Name:_____

Title: _____

Date: _____

ATTACHMENT 1

STANDARD CONTRACTUAL CLAUSES

Controller to Processor

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 personal data to a third country.

(b) The Parties:

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

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

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

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

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

Clause 2

Effect and invariability of the Clauses

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

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

Clause 3

Third-party beneficiaries

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

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

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

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

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

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clauses 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

Docking clause

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

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

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

MODULE TWO: Controller to Processor

8.1 Instructions

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

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

8.2 Purpose limitation

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

8.3 Transparency

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

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

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

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

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

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

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data

relating to criminal convictions and offences (hereinafter “sensitive data”), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

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

MODULE THREE: Processor to Processor

8.1 Instructions

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

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict

with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

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

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

8.2 Purpose limitation

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

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing

can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

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

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

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

8.7 Sensitive data

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

8.8 Onward transfers

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

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

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

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

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

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

8.9 Documentation and compliance

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

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

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of

the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

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

Clause 9

Use of sub-processors

MODULE TWO: Controller to Processor

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

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

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to

protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

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

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

MODULE THREE: Processor to Processor

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

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

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

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

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

Clause 10

Data subject rights

MODULE TWO: Controller to Processor

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

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking

into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

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

MODULE THREE: Processor to Processor

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

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

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

Clause 11

Redress

(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.

(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.

(f) The Parties agree that those shall be the courts of Ireland.

(g) 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.

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

APPENDIX TO ATTACHMENT 1 - STANDARD CONTRACTUAL CLAUSES

Annex I – Details of Processing

A. List of Parties

Data Exporter:

Customer's Name: _____
Customer's Address: _____
Contact Person Name: _____
Contact Person Title: _____
Contact Email: _____
Contact Phone: _____

Activities relevant to the data transferred under these Clauses: Processing of Personal Data in connection with Customer's use of the FME Cloud Online Services.

Signature & Date: Each party's signature of the DPA shall be considered a signature to these clauses.

Role: (select one) _____Controller _____ Processor

Data Importer:

Name: Safe Software Inc.
Address: Suite 1200, 9639 137a Street, Surrey, BC, Canada V3T 0M1
Contact Person Name: Angela McGeachan
Contact Person Title: Privacy Officer
Contact Email: privacy@safe.com
Contact Phone: 1-604-501-9985

Signature & Date: Each party's signature of the DPA shall be considered a signature to these clauses.

Role: Processor

B. Description of Transfer

Categories of Data Subjects whose Personal Data is Transferred

The categories of Data Subjects are solely determined and controlled by the Customer and may include, but are not limited to, Customer's employees, constituents, customers, partners, or vendors.

Categories of Personal Data Transferred

The categories of Personal Data are solely determined and controlled by the Customer and may include, but is not limited to, contact information and location data.

Sensitive Data Transferred

The parties do not anticipate the transfer of sensitive data.

Frequency of the Transfer

The frequency of the transfer depends on the frequency at which Customer uses the Online Services. It is expected that transfers will be periodic and ongoing.

Nature of the Processing

Data integration accomplished through a variety of operations as specified by the Customer's choice of actions. Operations include, but are not limited to, collection, translation, transformation, organization, structuring, use, dissemination, scheduling, combination, restriction, deletion, etc.

Purposes of the Data Transfer and Further Processing

Safe Software shall process Personal Data on behalf of and in accordance with Customer's documented instructions for the following purposes: (i) to provide the Online Services and any related technical support; (ii) as further specified via Customer's use of the Online Services (including any settings and other functionality of the Online Services); (iii) as documented in the Terms; and (iv) to comply with other documented reasonable instructions provided by Customer and acknowledged by Safe Software.

Period for which Personal Data will be Retained

Personal Data processed using the Online Services will be retained for 40 days after the Customer closes their Online Services account.

C. Competent Supervisory Authority

For the purposes of the Standard Contractual Clauses, the supervisory authority that will act as competent supervisory authority will be determined in accordance with the GDPR.

Annex II – Security Measures

Safe Software will maintain administrative, physical, and technical safeguards to protect the security, integrity, and confidentiality of Personal Data processed using the Online Services.

Our Security Statement, available at https://www.safe.com/legal/security-statement/, provides a summary of our organizational measures to ensure the security of your data.

The FME Cloud Security Whitepaper, available at https://community.safe.com/s/article/fme-cloud-security-faqs, provides a summary of technical measures.

Annex III – Sub-Processors

See https://www.safe.com/legal/gdpr/ for a list of all current Sub-Processors.

The list of Sub-Processors will be updated as changes occur. To subscribe to advance notification of any such updates please contact privacy@safe.com. Customer may object to such updates within 14 days from receiving an email notification or from the date that any updates were made to https://www.safe.com/legal/gdpr/, whichever is later. If the Customer objects to the proposed Sub-Processor and Safe Software cannot reasonably accommodate Customer's objection, then Safe Software will notify Customer and provide the Customer with the option to terminate the Online Services and receive a prorated refund of all prepaid amounts for the period after such termination date.

ATTACHMENT 2

INTERNATIONAL DATA TRANSFER ADDENDUM SCHEDULE

Purpose. This Schedule supplements the DPA entered into between the parties to govern the international transfer of personal data.

PART 1: TABLES

TABLE 1		
Start date	Upon final signature of the DPA	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	See Annex I.A to the SCCs	See Annex I.A to the SCCs
Key Contact	See Annex I.A to the SCCs	See Annex I.A to the SCCs
Signatures	Each party's signature of the DPA shall be considered a signature to this Schedule.	Each party's signature of the DPA shall be considered a signature to this Schedule.

TABLE 2	
Addendum EU SCCs	The version of the Approved EU SCCs which this Addendum is appended to including the Appendix Information.

TABLE 3	
Appendix Information means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:	
Annex 1A	List of Parties: As described in Annex I.A to the SCCs
Annex 1B	Description of Transfer: As described in Annex I.B to the SCCs
Annex II	Technical and organizational measures including technical and organizational measures to ensure the security of the data: As described in Annex II to the SCCs
Annex III	List of Sub-processors: As described in Annex III to the SCCs

TABLE 4	
Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: Importer

PART 2: MANDATORY CLAUSES

Mandatory Clauses	Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.