DRAGOS DATA PROCESSING AGREEMENT ("DPA")
Last Updated January 6, 2023

1. BACKGROUND AND DETAILS OF THE DATA PROCESSING

1.1 This DPA applies only to the extent Dragos processes Personal Data on behalf of Customer under Applicable Law. To the extent applicable, this DPA (including its Schedules) shall form part of the Agreement between Dragos and Customer and shall continue in force for as long as Dragos processes Personal Data on behalf of Customer. This shall include in particular, but not be limited to, the processing of the categories of Personal Data relating to the data subjects and for the purposes as listed in **Schedule 1** to this DPA.

1.2 The scope and duration, as well as the extent and nature of the collection, processing and use of Personal Data under this DPA shall be as defined in the Agreement.

2. DEFINITIONS

In addition to the definitions set out in the Agreement, the following definitions shall apply in this DPA:

"**Applicable Law**" means any laws that regulate the processing, privacy or security of Personal Data and that are directly applicable to each respective party to this DPA in the context of Dragos processing Personal Data, including, but not limited to, the General Data Protection Regulation 2016/679 ("**GDPR**") and any local laws implementing or supplementing the GDPR.

"**DPA**" means this Data Processing Agreement.

"**EEA**" means the European Economic Area.

"**EU Standard Contractual Clauses**" means the clauses attached as **Schedule 4** to this DPA, or (if applicable) any future clauses issued by the EU for the transfer of Personal Data to non-EU (sub)processors, and replacing or modifying the clause in the wording as issued by the EU, or any other clauses mutually agreed by the parties. In case of such modification or replacement, the **Schedules 1, 2 and 3** to this DPA shall remain schedules to the EU Standard Contractual Clauses.

"**Personal Data**" means personal data as defined in the GDPR and to the extent processed by Dragos on behalf of Customer when providing Offerings under the Agreement.

"**Restricted Transfer**" means any export of Personal Data from its country of origin to a third country in the course of Dragos's provision of the Offerings set forth in the Agreement that is prohibited under Applicable Law, unless (a) the destination has been recognized as providing an adequate level of data protection by competent data protection authority, or otherwise in a legal binding way, or (b) the parties adhere to an appropriate, under Applicable Law, recognized adequacy mechanism ensuring an adequate level of data protection.

"**Security Breach**" a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed by Dragos through the Offerings described in the Agreement.

Any terms used in this DPA, which are defined in the GDPR and not otherwise defined in this DPA, shall have the meaning as set out in the GDPR.

3. INSTRUCTIONS

3.1 Dragos will follow instructions received from Customer with respect to Personal Data.

3.2 Customer instructs Dragos to collect, process and use Personal Data to provide the Offerings as agreed in the Agreement.

3.3 Additional instructions with regard to the processing of Personal Data may be issued by Customer. Such instructions should be provided in advance and in writing by Customer, subject to Processor's right to charge additional sums at its current rates should the scope of the agreed Offerings be exceeded.

3.4 Dragos shall inform Customer if it considers an instruction to violate the GDPR or other EU or EU Member State data protection provisions.

4. OBLIGATIONS OF DRAGOS

4.1 Dragos shall not use the Customers' Personal Data for any purpose other than described in the Agreement and to fulfil its obligations under the Agreement unless required to do so by Applicable Law to which Dragos is subject; in such a case, Dragos shall inform Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

4.2 Dragos's personnel engaged in performing processing operations under this DPA have been bound to confidentiality and are prohibited from accessing, processing and/or using any Personal Data without authorization and for purposes other than fulfilling Dragos's contractual obligations vis-à-vis Customer.

4.3 Dragos will familiarize all individuals having access to the Customers' Personal Data with the data protection provisions relevant to their work.

4.4 Taking into account the nature of processing and the information available to Dragos, upon request and at Customer's expense, Dragos will assist Customer with its obligations under Articles 32 to 36 of the GDPR.

5. DATA SUBJECT'S RIGHTS

5.1 Taking into account the nature of the processing, upon request and at Customer's expense, Dragos will assist Customer with Customer's obligation to respond to requests from data subjects seeking to exercise their rights under the GDPR. Dragos may do so by implementing appropriate technical and organisational measures and by providing further assistance to the extent that such Personal Data is not already accessible to Customer through the Offerings.

5.2 Dragos will inform Customer without undue delay if a data subject contacts Dragos directly with a request as described in Articles 12 to 22 of the GDPR.

6. TECHNICAL AND ORGANIZATIONAL MEASURES

6.1 Dragos will implement and maintain the technical and organizational measures set out in **Schedule 2** to this DPA.

6.2 Upon Customer's request, Dragos will provide evidence of such technical and organizational measures through (i) current auditor's certificates, reports or excerpts from reports provided by independent bodies (e.g. auditor, Data Protection Officer, IT security department, data privacy auditor, quality auditor), or (ii) a suitable certification of IT security or data protection auditing (e.g. ISO/IEC 27001).

6.3 The technical and organisational measures are subject to technical progress and further development. Dragos may amend the technical and organizational measures, provided that the new measures do not fall short of the general level of security described in **Schedule 2**.

7. COMMUNICATION IN THE CASE OF PERSONAL DATA BREACHES

7.1 Dragos shall notify Customer without undue delay if Dragos becomes aware of any Security Breach. Notifications made pursuant to this section will describe, to the extent reasonably possible, details of the Security Breach, including steps taken to mitigate the potential risks and steps Dragos recommends the Customers take to address the Security Breach.

7.2 Customer instructs Dragos to take measures Dragos deems necessary or helpful to secure the Personal Data processed on behalf of Customer and to minimize possible adverse consequences to the data subjects.

8. INTERNATIONAL TRANSFERS

8.1 **Transfers from the European Economic Area**. The EU Standard Contractual Clauses in **Schedule 4** apply where (i) Personal Data is transferred, either directly or via onward transfer, from within the EEA to entities located outside of the EEA which are not recognized by the European Commission as providing an adequate level of protection for personal data; and where (ii) such transfer is not covered by a suitable framework recognized by the relevant EU data protection authorities, legislators or courts as providing an adequate level of protection for Personal Data (such as the EU-US Privacy-Shield). Any reference to Annexes I, II, and III in the EU Standard Contractual Clauses shall be read as reference to **Schedules 1, 2 and 3** of this DPA.

8.2 **Transfers from the United Kingdom**. Where Dragos makes a Restricted Transfer of Personal Data originating from the United Kingdom ("UK") to a third country not determined by the British Information Commissioner Office offering an adequate level of data protection, and where Dragos has not adopted another legally sufficient adequacy mechanism, the EU Standard Contractual Clauses in **Schedule 4** will be incorporated into this DPA and shall be read in accordance with, and deemed amended by, the provisions of Part 2 (Mandatory Clauses) of the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner under section 119A(1) Data Protection Act 2018 ("UK IDTA"). The parties confirm that the information required for the purposes of Part 1 (Tables) of the UK IDTA is set out in the relevant sections of **Schedules 1 and 2** of this DPA.

8.3 **Transfers from Switzerland**. Where Dragos makes a Restricted Transfer of Personal Data originating from Switzerland to a third country, the EU Standard Contractual Clauses in **Schedule 4** will be incorporated into this DPA and the following additional requirements shall apply to the extent that the data transfers are exclusively subject to the Swiss Data Protection Act ("FADP") or are subject to both the FADP and the GDPR: (i) The term 'member state' must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18 (c) of the EU Standard Contractual Clauses. (ii) Insofar as the data transfers underlying the EU Standard Contractual Clauses are exclusively subject to the FADP, references to the GDPR are to be understood as references to the FADP. Insofar as the data transfers underlying the EU Standard Contractual Clauses are subject to both the FADP and the GDPR, the references to the GDPR are to be understood as references to the FADP insofar as the data transfers are subject to the FADP.

9. SUBPROCESSING

9.1 Dragos may hire third parties to provide certain limited or ancillary services on its behalf, including those in **Schedule 3**. Customer consents to the engagement of these third parties and Dragos's affiliates as subprocessors.

9.2 From time to time, Dragos may engage new subprocessors. Dragos will give Customer notice of any new subprocessor at least fifteen (15) days in advance of providing that subprocessor with access to Customer or Personal Data.

9.3 If Customer does not approve of a new subprocessor, then Customer may terminate any subscription for the affected Service without penalty by providing, before the end of the relevant notice period, written notice of termination that includes an explanation of the grounds for non-approval.

9.4 Dragos shall remain responsible for its subprocessor's compliance with the obligations of this DPA and any subprocessor to whom Dragos transfers Personal Data, even those used for storage purposes, will have entered into written agreements with Dragos that provide at least the same level of protection as this DPA, in particular containing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that such subprocessing will meet the requirements of the GDPR.

10. AUDIT RIGHTS

10.1 The Customer may conduct an audit to verify Dragos's compliance with its obligations under this DPA if the Customer in its reasonable discretion believes that the right under section 6(b) of this DPA is not sufficient in an individual case, a competent data protection authority requests it, or the circumstances of a Security Breach require an earlier audit. Such audit may be conducted either by Dragos or by a third party auditor selected by Dragos, at Dragos's option. Dragos shall reasonably cooperate and provide such documentation and access as reasonably required to conduct the audit. For the avoidance of doubt, Dragos shall in no event be obliged to provide any information related to other customers. Dragos may claim remuneration for its efforts when enabling Customer audits, on a time and material basis and general rates in line with the market standard within this area.

10.2 Reasonable advance written notice of at least thirty (30) days is required for any such audit with Dragos, unless: (i) data protection law or a competent data protection authority require an earlier audit, in which case Dragos will be given as much advance notice as possible; or (ii) the circumstances of a Security Breach require an earlier audit, in which case Dragos will be given reasonable advance notice.

10.3 If an audit determines that Dragos has breached its obligations under this DPA, Dragos will promptly remedy the breach at its own cost.

10.4 The audits referred to in Clause 8.9(c)-(e) and Clause 13(b) of the EU Standard Contractual Clauses is bound by the terms for an audit as described in this section 10 of the DPA.

10.5 Upon reasonable request, Dragos will certify to the Customer that it is in compliance with this DPA by providing adequate evidence in the form of (i) the results of a self-audit, (ii) internal company rules of conduct including external evidence of compliance, (iii) certificates on data protection and/or information security (e. g. ISO 27001), (iv) approved codes of conduct, or (v) other appropriate certificates.

10.6 Evidence of the implementation of measures which are not specific to this DPA may be given in the form of up-to-date attestations, reports or extracts thereof from independent bodies (e.g. external auditors, internal audit, the data protection officer, the IT security department or quality auditors) or suitable certification by way of an IT security or data protection audit.

11. DELETION OF PERSONAL DATA

11.1 Following termination or expiry of the Agreement and upon first request by Customer, Dragos shall delete or return to Customer any Personal Data it processed for Customer under the Agreement. In absence of any such request, Dragos shall delete the Personal Data ninety (90) days after the aforementioned termination or expiry.

12. CALIFORNIA CONSUMER PRIVACY ACT

12.1 Dragos will comply with the California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 et seq., as amended by the California Privacy Rights Act (together, the "CPRA") as a "service provider" (as defined by the CPRA) in its provision of the Offerings under the Agreement. Terms used in this Section 12 not defined in this DPA or the Agreement will have the meaning assigned to them in the CPRA and its implementing regulations.

12.2 Dragos shall not (i) sell or share personal information; (ii) retain, use, or disclose personal information for any purpose other than for the business purposes specified in the Agreement, including retaining, using, or disclosing personal information for a commercial purpose other than the business purposes specified in the Agreement, or as otherwise permitted by the CPRA; (iii) retain, use, or disclose personal information outside of the direct business relationship between Dragos and Customer; or (iv) except as permitted to perform the Agreement or as otherwise permitted by the CPRA, combine the personal information that Dragos receives from, or on behalf of, Customer with personal information that it receives from, or on behalf of, another person or persons, or collects from its own interaction with a consumer.

13. MISCELLANEOUS

13.1 Dragos may amend this DPA where required to comply with any Applicable Law or where the amendments do not result in a material reduction in the protection of Personal Data and/or do not breach Applicable Law.

13.2 In the event of any contradictions between this DPA and the Agreement, the provisions of this DPA shall take precedence over the provisions of the Agreement.

DRAGOS

SCHEDULE 1

This Schedule forms part of the DPA.

A. LIST OF PARTIES

Data exporter(s):
The data exporter is: Customer

Name: As specified in the Agreement

Address: As specified in the Agreement

Contact person's name, position and contact details: Customer's contact details, as specified in the Agreement

Activities relevant to the data transferred under these clauses: Customer receives the applicable Offerings and related data processing services from Dragos as described in the Agreement. To enable this, Dragos may store and access Personal Data controlled by the Customer and which is contained in IT systems for which Dragos provides support to Customer.

Role: Controller

Data importer(s):
The data importer is: Dragos

Name: Dragos, Inc.

Address: 1745 Dorsey Road, Suite R, Hanover, MD 21076

Contact person's name, position and contact details: General Counsel, privacy@dragos.com

Activities relevant to the data transferred under these clauses: Dragos which renders the applicable Offerings and related data processing services.

Role: Processor

B. DESCRIPTION OF TRANSFER

Data subjects
The Personal Data may concern the following categories of data subjects:

- Employees and other staff of Customer
- Any other persons whose Personal Data are processed by Dragos on behalf of Customer.

Categories of data
The Personal Data may concern the following categories of data, where applicable:

- Machine and user logs
- Login credentials
- Contact details
- Any other Personal Data which are processed by Dragos on behalf of Customer

Sensitive data (if appropriate)
The Personal Data transferred concern the following sensitive data:

- None

Processing operations
The Personal Data may be subject to the following basic processing activities, where applicable:

- Security and IT support
- Hosting of dashboards and web applications

C. COMPETENT SUPERVISORY AUTHORITY

The data exporter's competent supervisory authority/ies will be determined in accordance with the GDPR.

SCHEDULE 2

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

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Dragos's administrative, physical, organizational and technical measures shall include, at a minimum, the following:

Documentation and accountability

Implementation of accountability principles and documentation of operations related to data processing and data security, This is accomplished through:

- Drafting, implementing and monitoring an extensive company-wide IT Security Policy and Standards for IT Assets; and
- Applying Confidentiality and Non-Disclosure Agreements where appropriate and as described in Dragos Policies.

Access control of processing areas

Implementation of suitable measures in order to prevent unauthorised persons from gaining access to the data processing equipment used to process the Personal Data. This is accomplished through:

- Keys and card key systems;
- building security; and
- CCTV.

Access control to data processing systems

Implementation of suitable measures to prevent data processing systems from being used by unauthorised persons. This is accomplished through:

- Individual user ID's and strong passwords subject to minimum security requirements for staff members;
- Mandatory password changes on regular intervals;
- Acceptable use policies for IT Assets such as PC's and mobile phones and applications;
- Strict on- and off-boarding policies for staff members;
- Lock out of user accounts after a limited number of failed log-in attempts; and
- Advanced firewalls, PEN testing, anti-virus and spam scanning.

Access control to use specific areas of data processing systems

The persons entitled to use its data processing systems are only able to access the data within scope and to the extent covered by their respective access permission (authorisation) and that the Personal Data cannot be read, copied or modified or removed without authorisation. This shall be accomplished by:

- Access management on strict need-to-know principles, job duties, project responsibilities and actual business activities; and
- Strict VPN corporate network requirements.

Transmission control

Implementation of suitable measures to prevent the Personal Data from being read, copied, altered or deleted by unauthorised parties during the transmission thereof or during the transport of the data media and to ensure that it is possible to check and establish to which bodies the transfer of Personal Data by means of data transmission facilities is envisaged. This shall be accomplished by:

- Firewall and encryption technologies to protect gateways through which the data travels; and
- Monitoring of encryption technologies.

Access and input control

Implementation of suitable measures to ensure that it is possible to check and establish whether, when, by whom and for what reason Personal Data have been input into data processing systems or otherwise processed. This shall be accomplished by:
Authentication of the authorised users via user ID and passwords;

- Restricted physical access to processing areas; and
- System time-out after non-activity for a pre-determined time period.

Instructional control

Personal data may only be processed in accordance with the DPA and Customer's instructions. This shall be accomplished by information & security training and policies & procedures for staff.

Availability control

Implementing suitable measures to ensure that Personal Data are protected from accidental destruction or loss. This shall be accomplished by:

- Backup and disaster recovery management; and
- Offsite backup storage.

Separation of processing for different purposes

Implementing suitable measures to ensure that Personal Data that are intended for different purposes can be processed separately. This shall be accomplished by:

- Access to Personal Data being restricted via user authorization passwords;
- Function separation of Personal Data of different customers; and
- Use of Personal Data being application specific.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter.

As set forth in section 9 of the DPA.

SCHEDULE 3

LIST OF SUBPROCESSORS

Customer consents to Dragos engaging the subprocessors found at: https://www.dragos.com/subprocessors/.

DRAGOS

SCHEDULE 4

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) ([i]) 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 ([ii]) (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) The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least fifteen (15) days prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ([iii]) 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 ([iv]) 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 ([v]);

(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 the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of The Republic 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 The Republic 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.

---

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

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

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

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

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