CYREBRO

# DATA PROCESSING ADDENDUM

This Data Protection Agreement ("**DPA**"), as amended from time to time, serves as an integral part of the Terms & Conditions (the "**Agreement**"), entered into by and between Cyber-Hat Ltd. or the Cyber-Hat Affiliate party, in accordance with the Agreement (together "**Cyber-Hat**") on behalf of itself and its Affiliates, and the counterparty of the Agreement, on behalf of itself and its Affiliates ("**Controller**"). Each of Cyber-Hat and Controller is referred to individually as a "**Party**" and collectively as "**Parties**".

## 1. Background.

1.1. In the course of exercising its obligations under the Agreement, Cyber-Hat processes personal data for or on behalf of the Controller;

1.2. By virtue of the Agreement and this DPA, Cyber-Hat may process Personal Data on behalf of the Controller.

## 2. Interpretation; Definitions.

2.1. Unless otherwise defined herein, capitalized terms used in this DPA shall have the following meaning:

| | |
|---|---|
| "**Affiliate**" | means any person or entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control" for the purpose of this definition means direct or indirect ownership or control of at least 50%. |
| "**Applicable Law(s)**" | means all applicable data protection and privacy and electronic marketing legislation, including Data Protection Act 2018, the EU Privacy and Electronic Communications (EC Directive) Regulation, the GDPR, the CCPA as well as any equivalent laws that may apply to the Controller's Personal Data to be processed hereunder by Cyber-Hat. |
| "**CCPA**" | means the California Consumer Privacy Act of 2018 California Civil Code § 1798.100 et seq., as supplemented or amended by the California Privacy Rights Act of 2020. Under the CCPA, Cyber-Hat qualifies as a service provider, and Cyber-Hat agrees to comply with the requirements of service providers as described in the CCPA and as specifically described in this DPA. |
| "**Cyber-Hat Services**" | means any services provided by Cyber-Hat to the Controller under the Agreement. |

| | |
|---|---|
| "**EEA**" | means European Economic Area. In this DPA the EEA shall include the EU Member States and EEA member countries. |
| "**GDPR**" | means EU General Data Protection Regulation 2016/679 and any subsequent amendments, replacements, or supplements; the terms "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Special Categories of Data**", "Process" or "Processing", "**Controller**", "**Processor**", and "**Supervisory Authority**" shall have the same meaning given to them in the GDPR (or where the same or similar terms are used under another Applicable Law, the meaning given to such terms under such Applicable Law. |
| "**Sensitive Personal Data**" | means a subset of Personal Data, which due to its nature has been classified by applicable law or by Cyber-Hat as deserving additional privacy and security protection. Sensitive Personal Data consists of, in particular:<br>(i) all government-issued identification documents and numbers (including Social Security numbers, driver's license numbers, and passport numbers);<br>(ii) all financial information, including any consumer, trading or spending habits, and any account numbers (bank and non-bank financial services account numbers, credit/debit card numbers, and other information would permit access to a financial account);<br>(iii) any Personal Data pertaining to the categories specified in Articles 9-10 of the GDPR;<br>(iv) all employee, employment candidate, and payroll information and data; and<br>(v) any other Personal Data designated by Cyber-Hat as Sensitive Personal Data. |
| "**Sub-Processors**" | means any Processor engaged directly by Cyber-Hat or any Cyber-Hat Affiliate to process any Personal Data pursuant to or in connection with the Agreement. The term shall not include employees or contractors of Cyber-Hat. |

3. **Scope of processing**.

3.1. The Controller hereby instructs Cyber-Hat to process Personal Data solely for the purpose of providing the Cyber-Hat Services, unless applicable laws to which Cyber-Hat is subject require such Processing. Cyber-Hat shall process Personal Data as a Data Processor acting on behalf of the Controller of such Personal Data.

3.2. Cyber-Hat shall process the Personal Data as described in **Annex 1** (details of Processing of Personal Data) attached hereto and in accordance with, (i) the terms of this DPA; (ii) the terms of the existing agreement between the Parties; (iii) the Controller's documented instructions, unless the processing is required by Applicable Laws; and (iv) all Applicable Laws.

3.3. Cyber-Hat shall notify the Controller without undue delay if Cyber-Hat determines that it can no longer meet the Controller's instructions or its obligations under this DPA.

3.4. The Controller warrants that its instructions at all times shall comply with applicable data protection and privacy legislation. The Controller furthermore warrants that it has an appropriate legal basis for the collection and processing of the Personal Data under this Agreement and DPA and is solely responsible for the legality of such Personal Data.

## 4. California Consumer Privacy Act (CCPA) / California Privacy Rights Act (CPRA)

4.1. To the extent any Controller Data is considered Personal Information (as such term is defined under the CCPA) and is subject to the CCPA, the parties agree that: (a) Cyber-Hat shall not sell or share (as those terms are defined in the CCPA and other applicable Protection Laws; (b) Cyber-Hat shall only use and process the Controller Personal Information on the Controller's behalf and solely pursuant to the terms set forth in the Agreement; (c) Cyber-Hat may engage in "Business Purposes" within the scope of the CCPA, including the Business Purposes as defined in Sections 1798.140 (2)-(7).

4.2. Cyber-Hat shall not (a) retain, use, or disclose Controller Personal Information for any purpose other than for the specific purpose of performing the Services or as otherwise expressly permitted under the Agreement including retaining, using or disclosing the Personal Information for a commercial purpose other than the business purposes specified in this DPA Terms or the Agreement, or as otherwise permitted by the CCPA; (b) retain, use or disclose the Controller Personal Information outside of the direct business relationship with the Controller; (c) combine the Controller Personal Information with personal information that it receives from or on behalf of a third party or collects from California residents, except that Cyber-Hat may combine the Controller Personal Information to perform any business purpose as permitted by this DPA, the Agreement, or the CCPA or any regulations adopted or issued under the CCPA.

4.3. Cyber-Hat shall assist the Controller to fulfill required obligations under the CCPA and to respond to requests from consumers exercising their rights under the CCPA (e.g., deletion and access), all in accordance with the CCPA requirements.

## 5. Cyber-Hat's Personnel.

Cyber-Hat shall take reasonable steps to ensure that all the Cyber-Hat's employees or contractors ("**Cyber-Hat Personnel**"): (i) have such access only as necessary for the purposes of providing the Cyber-Hat Services and is acting in compliance with Applicable

Laws; (ii) is contractually bound to confidentiality requirements no less onerous than this DPA; and (iii) is providing with appropriate privacy and security training, if and as required by Applicable Law.

## 6. Security.

6.1. Cyber-Hat shall assess and implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk presented by the processing of Personal Data, as described in **Annex 2**, including:

6.1.1. The pseudonymization and/or encryption of Personal Data, which in the case of any Sensitive Personal Data, shall be encrypted in transit and at rest;

6.1.2. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

6.1.3. The ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and

6.1.4. A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing.

6.2. In assessing the appropriate level of technical and organizational measures, Cyber-Hat shall take into consideration the risks that are presented by the Processing, including the risk of a Personal Data Breach, through accidental or unlawful loss, destruction, alteration, unauthorized disclosure of or access to the Controller's Personal Data.

6.3. Cyber-Hat shall keep records of its processing activities performed on behalf of the Controller, which shall include:

6.3.1. The details of the Processor as Personal Data Processor, any representatives, Sub-Processors and the Cyber-Hat Personnel having access to Personal Data;

6.3.2. The categories of Processing activities performed;

6.3.3. Information regarding cross-border data transfer, if any; and

6.3.4. Description of the appropriate technical and organizational security measures implemented in respect of the processed Personal Data.

## 7. Sub-processing.

7.1. Cyber-Hat has the Controller's authorization for the engagement of Sub-Processors as available at www.cyrebro.io/subprocessor. Cyber-Hat shall inform the Controller in writing of any changes to the list through the addition or replacement of the Sub-Processor within thirty (30) days following such changes (the "**Engagement**"). The Controller may reasonably object to the Cyber-Hat's use of a new Sub-Processor, for a reason relating to the protection of Personal Data intended to be processed by such Sub-Processor, by notifying Cyber-Hat promptly in writing within fourteen (14) days after the Cyber-Hat's notice.

7.2. Such written objection shall include those reasons for the objection to the Cyber-Hat's use of such a new Sub-Processor. Failure to object to the Engagement in writing and on a timely manner shall be deemed as acceptance of the new Sub-Processor. In the event the Controller reasonably objects to an Engagement, Cyber-Hat will use reasonable efforts to make available to the Controller a change in Cyber-Hat Services so to avoid processing of Personal Data by the Sub-Processor to which the Controller objects, without unreasonably burdening the Controller. If Cyber-Hat is unable to make available such change within thirty (30) days, the Controller Parties may, as a sole remedy, terminate the applicable agreement and this DPA with respect only to those services which cannot be provided by Cyber-Hat without the use of the Sub-Processor to which the Controller objected, by providing written notice to Cyber-Hat. The Controller will have no further claims against Cyber-Hat due to the termination of the Agreement and/or this DPA in the situation described in Article 7.

7.3. Where Cyber-Hat engages Sub-Processors, Cyber-Hat will take reasonable steps to impose on the Sub-Processors, by way of contract, data protection terms that provide at least the same material level of protection for Personal Data as those in this DPA (including, where appropriate, the Standard Contractual Clauses), to the extent applicable to the nature of the services provided by such Sub-Processors.

## 8. Data Subjects Rights.

8.1. The Controller is solely responsible for compliance with any obligations regarding the exercise of Data Subject Rights under applicable privacy legislation.

8.2. Taking into consideration the nature of the processing, Cyber-Hat shall reasonably assist the Controller in responding to requests to exercise Data Subject rights under Applicable Laws, including EU Data Protection Laws.

8.3. Cyber-Hat shall:

8.3.1. Promptly notify the Controller if it receives a request from a Data Subject in respect of Personal Data;

8.3.2. Provide cooperation and assistance where feasible in relation to any Complaint or request from a Data Subject regarding the Processing of Personal Data at the Controller's sole expense;

8.3.3. Ensure that it does not respond to that request except on the documented instructions of the Controller or as required by Applicable Laws to which Cyber-Hat is subject, in which case Cyber-Hat shall to the extent permitted by Applicable Laws inform Controller of that legal requirement before it responds to the request;

8.3.4. Maintain electronic records of complaints or requests from Data Subjects seeking to exercise their rights (under Applicable Laws).

## 9. Legal Disclosure; Personal Data Breach.

9.1. Cyber-Hat shall notify the Controller without undue delay of becoming aware of:

9.1.1. Any legally binding request for disclosure of Personal Data by a law enforcement authority unless otherwise prohibited by applicable laws and/or regulations;

9.1.2. a Personal Data Breach affecting Controller Personal Data, providing Controller with sufficient information (to the extent possible) to allow the Controller to meet any obligations to report or inform Data Subject or Data Protection Authorities of the Personal Data Breach under the Applicable Laws.

9.2. Cyber-Hat shall cooperate with the Controller and take reasonable commercial steps as directed by the Controller to assist in the investigation, mitigation and remediation of each such Personal Data Breach, all in accordance with the demands of the Applicable Law at the Controller's sole expense.

9.3. Other than as required by law, Cyber-Hat shall not make any public statements or other disclosures about a Personal Data Breach affecting Personal Data without the Controller's prior written consent, which is provided on a case-by-case basis.

## 10. Erasure or return Personal Data.

10.1. Within thirty (30) days after the termination of the Agreement, or at the Controller's written request, Cyber-Hat shall erase, return or otherwise make unrecoverable and/or anonymized all copies of Personal Data, at the Controller's choice, except as required to be retained or archived in accordance with applicable law and/or by the order of a governmental or regulatory entity. Provided, however, that (i) such Personal Data shall be maintained for as long as such legal requirement applies; and (ii) The Personal Data that remains in the possession of Cyber-Hat shall be subject to the same provisions of this DPA and shall be processed only as necessary for the purpose(s) specified in the applicable laws requiring its storage and for no other purpose.

10.2. Upon the Controller's prior written request, the Cyber-Hat's Data Privacy Officer or equivalent shall provide written certification to the Controller that it has fully complied with this section.

10.3. The obligations under this Article 10 shall remain in force even after the termination of this DPA.

## 11. Provision of information.

Cyber-Hat shall provide cooperation and assistance to the Controller, at the Controller's expense, with any data protection impact assessments, and prior consultations with relevant competent Data Privacy Authorities as required under Applicable Laws. The scope of such assistance shall be limited to the Processing of the Controller's Personal Data by Cyber-Hat.

## 12. Audit rights.

12.1. Cyber-Hat shall make available to the Controller, upon prior written request, not more than once a year, except in the event of a Personal Data Breach, information

necessary to demonstrate compliance with this DPA, including industry standard third-party audit certifications.

12.2. The Controller shall provide at least four (4) weeks prior written notice to Cyber-Hat of a request to audit.

12.3. Cyber-Hat shall allow for and contribute to audits, including inspections, by a reputable auditor mandated by the Controller, and agreed upon by Cyber-Hat. Such reputable auditor shall be paid by the Controller. The scope, duration, and methods of such an audit will be determined by the Parties in good faith. In any event, a third-party auditor shall be subject to confidentiality obligations and a non-disclosure agreement. Cyber-Hat may object to the selection of the auditor if it reasonably believes that an auditor does not guarantee confidentiality, security or otherwise puts at risk the Cyber-Hat's business. The Controller shall avoid causing any damage, injury or disruption of Cyber-Hat's premises, equipment, personnel, and business operations while performing the audit.

## 13. Cross-border data transfer.

13.1. Personal Data may be transferred from the country in which it originated to perform the Services for the Controller. The Controller shall obtain and maintain any and all necessary consents where applicable or ensure it has the right to allow for such transfer. Data transfers under the Agreement from the EEA, Switzerland and/or the United Kingdom to countries that do not offer an adequate level of data protection under or pursuant to the adequacy decisions published by the relevant data protection authorities of the EEA, the European Union, Member States or the European Commission, without any further safeguard being necessary or otherwise under Applicable Laws or another official certification body to the extent permitted under Applicable Laws, shall be subject to the Standard Contractual Clauses attached in **Annex 4** ("**SCCs**").

13.2. Unless Cyber-Hat transfers Personal Data according to 13.1, Cyber-Hat shall execute and abide by the SCCs attached in **Annex 5**, which shall apply to the processing of Personal Data in countries outside the UK that do not provide the aforementioned adequate level of data protection.

13.3. Where and to the extent that the SCCs are applicable, if there is any conflict between this DPA and the SCCs, the SCCs shall prevail.

13.4. In any event, Cyber-Hat shall provide the Controller with all relevant information to enable the Controller to comply with its obligations in case of cross-border transfers.

## 14. Term of the DPA.

The term of this DPA shall be the same as the term of the Agreement. Should any part of the Cyber-Hat Services continue after the termination or expiration of the Agreement, then the provisions of this DPA shall continue to govern such services and for that purpose, this DPA shall remain in force and effect as long as such Cyber-Hat Services are rendered by Cyber-Hat.

15. **Liability and indemnification.**

15.1. The "*limitation of liability*" provisions as set forth in Section 13 to the Agreement shall apply to this DPA.

15.2. To the extent Cyber-Hat shall be subject to any enforcement action or any third-party claim, based on any acts or omissions of the Controller relating to the end user's Personal Data, or any failure by the Controller to comply with any applicable Data Protection Laws, the Controller shall hold Cyber-Hat harmless and fully indemnify Cyber-Hat at its first demand, for any expenses, losses and damages, including without limitation, reasonable attorney's fees and any fines and levies, incurred by Cyber-Hat in connection with and as a result of such enforcement action or claim.

16. **Miscellaneous**.

16.1. Severance. If any provision or any part thereof contained in this DPA is, for any reason, held to be invalid, or unenforceable in any respect under the laws of any jurisdiction where enforcement is sought, such invalidity or unenforceability will not affect any other provision of this DPA and the remainder of the DPA will remain in force. The DPA will be construed as if such invalid or unenforceable provision or part thereof had never been contained therein, or shall be amended as needed to ensure its validity and enforceability.

16.2. Jurisdiction. This DPA shall be governed by and construed in accordance with the laws of the State of Israel. Any dispute arising out of or in connection with this DPA shall submit to the exclusive jurisdiction of the competent Courts of Tel Aviv – Jaffa, Israel.

16.3. Notice. All notices required under this DPA shall be sent to each Party to the addresses as detailed in the Agreement.

16.4. Order of precedence. In the event of any conflict between the terms of this DPA and other documents binding on Parties, the terms of these documents will be interpreted according to the following order of precedence: (i) the SCCs (as applicable); (ii) this DPA; (iii) the Cyber-Hat's Privacy Policy as published at the Cyber-Hat's website; and (iv) terms of any agreement, order form, purchase order, license of subscription, pursuant to which Cyber-Hat's Services are provided.

IN WITNESS WHEREOF, this DPA is entered into and becomes binding between the Parties with effect from the date first set out above.

**Annexes**:

The following annexes are integral parts of this DPA:

Annex 1: List of parties; Description of transfer.

Annex 2: Technical and Organizational measures including technical and organizational measures to ensure the security of the data.

Annex 3: Standard Contractual Clauses - EU

Annex 4: Standard Contractual Clauses - UK

Annex 1

This Annex 1 includes certain details of the Processing of Personal Data.

## A. List of Parties

### Data exporter(s):

Role: Controller

### Data importer(s):

1. Name: Cyber-Hat Ltd.

Address: 52 Menachem Begin St., Tel Aviv, Israel

Contact person's name, position and contact details: CYREBRO Legal Team, legal@cyrebro.io

Signature: Nadav Arbel, CEO, 1/1/2023

Role: Processor

## B. Description of transfer

1. *Categories of data subjects whose personal data is transferred*: The group of individuals affected by the processing of Personal Data under the Agreement may include the Controller's employees, subcontractors and other persons who are able to create log sources of information in the Controller's security systems.
2. *Categories of personal data transferred*: The types of Personal Data that may be collected, processed and/or used under the Agreement may include the following: first and last names, email addresses, phone numbers, usernames, passwords, IPs, photos, and documents. In the normal course of business, the Processor should not have access to any information other than the log sources information moderated.
3. *Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures*: None.
4. *The frequency of the transfer*: *On a continuous basis.*
5. *Nature of the processing*: The data processing is an inseparable part of the Security Operating Center ("**SOC**") services, as the Controller provides the Processor with access to its log sources information for the purpose of providing ongoing monitoring services and alerting and researching any suspicious activity.
6. *Purpose(s) of the data transfer and further processing*: the Processor operates a SOC, from which it monitors the Controller's security system pursuant to the Controller's preferences. The data is processed as a by-product of the Processor's

solution, as in many of the cases the providence of the services includes an interface with data stored on the Controller's database. If the data is relevant for providing the monitoring services, it might be saved by the Processor on local servers or appear in the Processor's report prepares for the Controller as part of the Processor Services.

With respect to the stored data – some data collected is stored in cloud-based storage provided by the below Sub-processors:

https://www.cyrebro.io/subprocessors/

## Annex 2 – Technical and Organizational measures including technical and organizational measures to ensure the security of the data

*Description of the technical and organizational 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.*

The Processor is compliant and will remain compliant throughout the terms of the Agreement and this DPA, with ISO 27001 and ISO 22301, and therefore has implemented all the technical and organizational security requires measures.

**Measures to ensure confidentiality**:

1. Physical access control. Measures that physically deny authorized person access to IT systems and data processing equipment used to process Personal Data, as well as to confidential files and data storage media. Physical access control information is implemented according to ISO 27001 requirements and according to best practices.
2. Logical access control. Measures to prevent unauthorized persons from processing or using Personal Data that is protected by applicable privacy laws. Logical access control is implemented according to ISO 27001 requirements and according to best practices.
3. Separation rule. Measures to ensure that Personal Data collected for different purposes are processed separately and separated from other data and systems in such a way as to unplanned use of such data for other purposes. Separation rule and separation control process implemented according to ISO 27001 requirements and according to best practice.

**Measures to ensure integrity**:

1. Data integrity. Measures to ensure that stored Personal Data cannot be corrupted by means of a malfunctioning of the system. Data integrity measures are implemented according to ISO 27001 requirements and according to best practices.
2. Transmission control. Measures to ensure that it is possible to verify and establish to which bodies the Personal Data may be or have been transmitted or made available using data communication equipment. The transmission control is implemented according to ISO 27001 requirements and according to best practices.
3. Transport control. Measures to ensure that the confidentiality and integrity of the Personal Data are protected during transmission of Personal Data and transport of data carriers. The transport control is implemented according to ISO 27001 requirements and according to best practices.
4. Input control. Measures to ensure that it can be subsequently verified and ascertained whether and by whom Personal Data has been entered or modified in data processing systems. The Processor monitors access to its systems upon which Personal Data is processed and maintains logs of such access to its systems which shall include the following information: User identity, data and time of access attempt, system

component to which access was attempted, access type, its scope, and whether access was granted or denied (the "**Log Data**"). The Log Data shall be retained by the Processor for at least 24 months and provided to the Controller upon request. The input control is implemented according to ISO 27001 requirements and according to best practices.

**Measures to ensure availability and resilience**

1. Availability control. Measures to ensure Personal Data is protected against accidental destruction or loss or unauthorized access.
2. Quick recovery. Measures to ensure the ability to quickly restore the availability of and access to Personal Data and used systems in the event of physical or technical incidents.
3. Reliability. Measures to ensure that the functions of the system are available and implemented according to ISO 22301 requirements and according to best practices.

**Measures for the regular testing and evaluation of the security of data processing**

1. Verification process. Measures to ensure that the data are processed securely and in compliance with data protection regulations. Such process is done via documentation of instructions received by the Controller. The Processor will conduct penetration testing of its systems every eighteen (18) months from the date of the Agreement. The Processor will perform a vulnerability and security assessment every eighteen (18) months from the date of the assessment, whether by its own qualified personnel or through a certified provider, the Processor will share the results with the Controller. Any non-compliance shall be promptly corrected by the Processor.
2. Order control. Measures to ensure that Personal Data processed on behalf of the Controller can only be processed in accordance with the instructions of the Controller.

## Annex 3 – Standard Contractual Clauses - EEA

### Section I

*Clause 1*

### *Purpose and Scope*

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b) The Parties:

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

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

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

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

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

*Clause 2*

### *Effect and invariability of the Clauses*

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update

---

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 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 […].

information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

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

*Clause 3*

*Third-party beneficiaries*

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

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

(ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

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

*Clause 4*

*Interpretation*

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

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

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

*Clause 5*

*Hierarchy*

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

*Clause 6*

*Description of the transfer(s)*

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

*Clause 7*

*Docking clause*

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

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

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

**Section II – Obligations of the Parties**

*Clause 8*

*Data Protection Safeguards*

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

**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 Onwards 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[2] (in the same country as the data importer or in

[2] 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

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***

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.

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

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.3 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

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

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.

(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) 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.

(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 safeguards4;

(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

---

4 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.

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 [for Module Three: , if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

*Clause 15*

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

**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 Ireland.

*Clause 18*

### *Choice of forum and jurisdiction*

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

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

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

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

## Annex I

### A. List of Parties

As detailed in Annex 1 to this DPA, or as detailed in specific Agreement between the Parties.

### B. Descirption of transfer

### C. Competent supervisory ahtorit

## Annex II – Technical and Organizational measures including technical and organizational 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.*

As detailed in Annex 2 to this DPA

## Annex III – List of Sub-processors

The controller has authorised the use of the following sub-processors:

https://www.cyrebro.io/subprocessors/

## Annex 4 – Standard Contractual Clauses - UK

## Table 1: Parties

As detailed in Annex 1 to this DPA, or as detailed in specific Agreement between the Parties.

## Table 2: Selected SCCs, Modules and Selected Clauses

| | |
|---|---|
| **Addendum EU SCCs** | ☐ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information:<br>Date: |

| | |
|---|---|
| | Reference (if any):<br>Other identifier (if any):<br>Or<br>X the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum: |

| Module | Module in operation | Clause 7 (Docking Clause) | Clause 11 (Option) | Clause 9a (Prior Authorisation or General Authorisation) | Clause 9a (Time period) | Is personal data received from the Importer combined with personal data collected by the Exporter? |
|---|---|---|---|---|---|---|
| 1 | | | | | | |
| 2 | X | X | | General Authoriation | 30 | |
| 3 | | | | | | |
| 4 | | | | | | |

**Table 3 – appendix Information**

All as attached as Annexes to this DPA.

**Table 4 – Ending this Addendum when the Approved Addendum Changes**

| | |
|---|---|
| **Ending this Addendum when the Approved Addendum changes** | Which Parties may end this Addendum as set out in Section **Error! Reference source not found.**:<br>☐ Importer<br>☐ Exporter<br>X neither Party |