Quasr BV

DATA PROCESSING ADDENDUM

This Quasr Data Processing Addendum ("**DPA**") is entered into by and between Quasr BV, a limited liability company (*besloten vennootschap* or *BV*) incorporated, organized and existing under the laws of Belgium, with registered office at New Yorkkaai 85, bus 302, 2000 Antwerpen (Belgium) and registered with the Crossroads bank of Enterprises (*Kruispuntbank van Ondernemingen* or *KBO*) under enterprise number 0779.655.316 (hereinafter referred to as the **"Processor"** or **"Quasr"**) and the entity identified as such in the applicable Order Form (hereinafter referred to as the **"Controller"** or **"Customer"**). The Customer and Quasr are hereinafter individually referred to as a **"Party"** jointly as the **"Parties"**.

1. INTRODUCTION

Pursuant to the Quasr Subscription Agreement, the Controller was granted access to the Quasr Platform. Through the Quasr Platform, Personal Data is collected and processed by the Processor on behalf of the Controller. The Parties wish to enter into a DPA in accordance with the requirements of applicable Data Protection Legislation, including the GDPR. This DPA forms part of the Quasr Subscription Agreement. The attached Schedules form an integral part of this DPA.

By indicating Controller's acceptance of this DPA, or by executing a "Sales Order" under an agreement that references this DPA, Controller agrees to be bound by this DPA. If the signatory is entering into this DPA on behalf of an entity, such as the company you work for, then you represent to Quasr that you have the legal authority to bind the Controller to this DPA. If the signatory does not have that authority or if Controller does not agree with the terms of this DPA, then the signatory may not indicate acceptance of this DPA. This DPA is effective between Controller and Processor on the date on which Customer indicates its assent to the DPA.

This DPA replaces previous provisions in past and current agreements between the Parties that are directly or indirectly related to the processing of personal data, privacy, access to personal data, data transfers and data security. In case of contradictions between the conditions of the Quasr Subscription Agreement and this DPA, the conditions of this DPA shall prevail. In case of contradictions between this DPA without the Schedules and the Schedules, the conditions in the Schedules shall prevail.

2. DEFINITIONS

Capitalized terms used in this DPA shall be interpreted as defined in this section or elsewhere in the DPA. Capitalized terms not defined herein shall have the meaning given to them in the Quasr Subscription Agreement, unless the context requires otherwise. In case of doubt or differences with the terms defined in the GDPR, the definitions set forth in the GDPR shall prevail. Clause headings shall not affect the interpretation of this DPA and the words "include" and "including" shall not limit the generality of any words preceding them. In addition to the terms defined herein, the following terms shall be defined as follows:

"Applicable Data Protection Laws"	means the EU Regulation 2016/679 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), together with the codes of practice, codes of conduct, regulatory guidance and standard clauses and other related legislation resulting from such Directive or Regulation, as updated from time to time.
"Controller"	means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

"Data Subject"	means an identified or identifiable natural person to whom the Personal Data relates. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. The relevant categories of Data Subjects are identified in Schedule 1.
"GDPR"	means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (known as the General Data Protection Regulation).
"Personal Data"	means any information relating to an identified or identifiable natural person and to an identified or identifiable entity, which is processed by the Processor solely on behalf of the Controller, as part of the Services under the Quasr Subscription Agreement.
"Personal Data Breach"	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed in connection with the provisioning of the Quasr Platform.
"Processing", Process(es)" or **"Processed"**	means any operation or set of operations which is performed upon Personal Data or on sets of Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
"Processor"	means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller
"Quasr Subscription Agreement"	means applicable subscription and license agreement entered into between the Customer and Quasr with respect to the use of the Quasr Platform (i.e. Self Service Terms of Service or Quasr Enterprise Subscription Agreement).
"Security Measures"	means the technical and organizational security measures to be applied by Processor in respect of the Personal Data.
"**SCCs"**	means where the GDPR applies, the standard contractual clauses annexed to the European Commission's Decision (EU) 2021/914 of 4 June 2021 ("**EU SCCs**").
"Sub-processor"	means any subcontractor engaged by Quasr to perform a part of the Services and who agrees to receive Personal Data intended for Processing on behalf of the Customer in accordance with the Customer's instructions and the provisions of the Agreement

3. PROCESSING OF PERSONAL DATA

1. The Parties acknowledge that Quasr acts as Processor with respect to the Personal Data as a result of the performance of the Quasr Platform. The Customer remains at all times the Controller with respect to the Personal Data.

2. Each of the Parties shall comply with its respective obligations in relation to the Processing of Personal Data under the Applicable Data Protection Laws.

3. During the use of the Quasr Platform, the Customer may provide certain Personal Data to Quasr for Processing. Quasr will only Process such Personal Data during the term of the Quasr Subscription Agreement or for another agreed period (e.g. in the event of early termination), and in no case will it keep the Personal Data longer than is necessary in function of the purpose for which they are Processed.

4. A more detailed description of the subject matter of the Processing of Personal Data in terms of the concerned categories of Personal Data and Data Subjects is contained in Schedule 1 hereto.

4. OBLIGATIONS OF CUSTOMER

1. Processor will only process the Personal Data in order to provide the Quasr Platform and will act only in accordance with the Agreement and Customer's written instructions. The Quasr Subscription Agreement, this DPA, and Customer's use of the Quasr Platform's features and functionality, are Customer's written instructions to Quasr in relation to the processing of Personal Data.

2. If Quasr is required to Process or transfer Personal Data to a third country or an international organization pursuant to a provision applicable to it, Quasr shall notify the Customer of such legal provision, unless such legislation prohibits such notification.

3. Under this DPA and pursuant to the use of the Quasr Platform, the Customer is responsible for compliance with all obligations to which the Customer is subject under Applicable Data Protection Laws, in particular with respect to the Processing of Personal Data.

4. Without prejudice to the foregoing, the Customer agrees in particular that it is solely responsible: (i) for the accuracy, quality and lawfulness of Personal Data and of the manner in which the Customer has obtained such Personal Data; (ii) for compliance with all obligations of transparency and lawfulness contained in the Applicable Data Protection Laws regarding the collection and use of the Personal Data; (iii) and that it has the right to provide the Personal Data to Quasr and to grant Quasr access for Processing in accordance with the provisions of the Quasr Subscription Agreement; and (iv) that its instructions to Quasr regarding the Processing of Personal Data comply with applicable law, including the Applicable Data Protection Laws. The Customer shall notify Quasr without unreasonable delay if it is unable to comply with its obligations under this Article or under the Applicable Data Protection Laws.

5. Nothing in this DPA shall constitute a right to use (or allow others to use) the Quasr Platform for any unlawful purpose or in any manner other than as contemplated in the Quasr Subscription Agreement and/or in this DPA

5. CONFIDENTIALITY

The Processor shall ensure that persons authorized by it to process the Personal Data are bound by enforceable confidentiality obligations not to disclose it and shall inform any person who has access to the Personal Data (including employees, temporary workers and independent contractors) of the obligations of Quasr with respect to the Customer's Personal Data.

6. TECHNICAL AND ORGANIZATIONAL MEASURES

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of the Data Subjects, Processor will implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks that are presented by the processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data in Quasr's possession or under its control, in such a manner that the Processing of Personal Data will meet the requirements of the Applicable Data Protection Laws and ensure the protection of the rights of each Data Subject. Customer acknowledges that Quasr security measures are designed to ensure a level of security appropriate to the risk. Customer further acknowledges that it is responsible for its configuration of

the Quasr Platform and for using features and functionality of the Quasr Platform to ensure a level of security appropriate to the risks presented by the processing. A more detailed description of the different technical and organizational measures of the Processor is contained in Schedule 3 hereto.

2. Processor shall take account of the risks that are presented by Processing the Personal Data in assessing the level of security required for Personal Data.

7. INFORMATION OBLIGATIONS AND ASSISTANCE

1. Processor shall make available to Controller all information reasonably necessary to demonstrate compliance with this DPA and shall allow for and contribute to audits, including inspections, conducted by Controller, or another auditor mandated by Controller on ten (10) working days' notice and mutual agreement of a suitable scope and agenda. The Controller shall limits its initiatives to conduct an audit or inspection no more than once per year except in the event that (i) it is required to do so by law, (ii) Processor has experienced a Personal Data Breach in the preceding twelve (12) months that has affected Controller's Personal Data or (iii) in the case of a mutual agreement. The Controller shall ensure that the audit is conducted in such a way that the inconvenience for the Processor is kept to a minimum. The Controller shall impose adequate confidentiality obligation on its auditors. In addition, the Processor may require that the Controller and its auditors to enter into a confidentiality agreement prior to the commencement of the audit.

2. The scope of an audit may not result in an obligation to give or provide to the auditor access to: (a) information or data of any other customer of Quasr; (b) trade secrets of Quasr or related information; (c) any information which, in Quasr's reasonable opinion, may compromise the security of Quasr's systems or premises or which may cause Quasr to breach its obligations under Applicable Data Protection Laws or other security, confidentiality or privacy obligations to other customers of Quasr or to third parties or (d) any information that the auditor wishes to inspect for reasons other than the good faith performance of its obligations under the Applicable Data Protection Laws and Quasr's compliance with the provisions of this DPA. The Controller will bear all the costs for such an audit or inspection.

3. Processor shall immediately inform Controller if it becomes aware that Controller's processing instructions infringe the Applicable Data Protection Laws but without obligation to actively monitor Controller's compliance with them. Processor has the right to suspend the implementation of such instruction and not to further Process the Personal Data in accordance with instructions previously provided, following such notification. Such suspension shall not result in any right to compensation on the part of the Controller.

4. Processor shall assist the Controller in fulfilling its duty to respond to requests from Data Subjects for the exercise of their rights:

   - by notifying the Controller of all requests received relating to Personal Data from a Data Subject, a supervisory authority and/or any other authority competent for the Applicable Data Protection Laws;

   - by providing reasonable cooperation to the Controller in responding to requests from the Data Subject in accordance with the GDPR, but after obtaining the Controller's approval;

   - by ensuring that the Processor has the technical and organizational capabilities to remove the Personal Data of the Data Subject who requests such right from the Data Subject's system, records or databases. Personal Data may remain present on backup or archival media that are securely isolated and shielded from further Processing and then permanently deleted in accordance with the retention period policy.

5. In the event Processor becomes subject to a request from a public authority to disclose any Personal Data, Processor shall review the legality of such a request prior to acceding to it. To the extent permitted by law, Processor shall promptly notify Controller in writing of any such request. Processor shall only comply with such requests in the event that it reasonably considers that it is lawfully compelled to do so. Processor shall in respect of any such request (i) only disclose the minimum amount of Personal Data required, and (ii) retain evidence that any disclosure of

Personal Data to public authorities was made in accordance with the restrictions under this paragraph, and (to the extent permitted by law) make such evidence available to Controller promptly upon request.

6. Notwithstanding the foregoing, the Controller shall remain responsible for the proper handling of such requests by Data Subject

7. In the event that there is a confirmed Personal Data Breach in respect of the Personal Data provided by Controller, Processor shall without undue delay (and in any event within 72 hours of confirming such breach) notify Controller of that data breach in writing including the following details:

   a. the nature of the Personal Data Breach including the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;

   b. the likely consequences of the personal data breach; and

   c. the measures which Processor proposes to take to remediate the cause of the breach.

8. In the event of a Personal Data Breach in respect of the Personal Data provided by Controller, Processor shall provide Controller with such reasonable cooperation and assistance with managing that Personal Data Breach as may be agreed between the Parties, acting in good faith.

8. SUB-PROCESSING

1. Controller authorizes Processor to engage Sub-processors to process the Personal Data. The current list of Sub-processors for the Quasr Platform is attached as Schedule 2 to this DPA. Processor provides reasonable prior notice before the proposed addition or replacement of any Sub-processor by posting details at quasr.io/legal/sub-processors/, in order to allow Controller to raise in writing any reasonable objections on grounds of data protection within thirty (30) calendar days of such notice. In the event of such an objection, the Parties will discuss Controller's concerns in good faith with a view to achieving a commercially reasonable resolution. If no such resolution can be reached, Processor will, at its sole discretion, either not appoint the new Sub-processor, or permit Controller to suspend or terminate the Quasr Subscription Agreement without liability to either Party. Processor shall not be obliged to make any refund of any sums paid under the Quasr Subscription Agreement. The Controller bears the costs for all the consequences including but not limited to adjustments in the functioning of the Quasr Platform, when there is an objection to changes concerning the addition or replacement of a Sub-processor.

2. The Processor shall keep an up-to-date record of the agreements with Sub-processors and may provide it to the Controller upon simple request within a reasonable period of time.

3. If a Sub-processor fails to comply with its data protection obligations, the Processor will remain liable to the Controller for compliance with those obligations.

4. Controller acknowledges that Processor may be restricted from disclosing to Controller its contract terms with Sub-processors due to confidentiality obligations.

5. Processor shall ensure each Sub-processor is appointed under a binding written contract conferring a materially similar level of obligation on the Sub-processor in relation to protection of the Personal Data as under this DPA (including those relating to sufficient guarantees to implement appropriate technical and organizational measures) and shall be responsible for ensuring each such Sub-processor complies with all such obligations.

9. DELETE AND RETURN

1. Processor shall upon termination or expiry of the Quasr Subscription Agreement delete or return to Controller all Personal Data processed under this DPA (including any copies of it) unless (i) Quasr is required to retain the Personal Data pursuant to applicable law, or (ii) the Personal Data is archived in a back-up system which is kept by Quasr in a secure manner, is protected from further Processing and whereby Personal Data is deleted in accordance with Quasr's data retention policy.

2. Quasr will return Personal Data to Customer by permitting Customer to export Personal Data from the Quasr Platform at any time during provision of the Quasr Platform, using the Quasr Platform's then existing features and functionality. Customer may delete Customer Data on its Tenants at any time. ("**Tenant**" means a logical isolation unit, or dedicated share of a particular Quasr Platform instance; the dedicated share may be configured to reflect the needs of the specific Customer business unit using the share.) Quasr will delete Customer's Tenants (and any data remaining on such Tenants) within thirty (30) calendar days of termination or expiration of the Subscription Term, and other Personal Data retained by Quasr (if any). Quasr will keep the Personal Data as long as necessary for the purpose of executing the Quasr Subscription Agreement or when it may be required by law, or as otherwise communicated to you. How long we retain specific personal information varies depending on the purpose for its use, and we will delete your personal information in accordance with applicable law.

10. DATA TRANSFERS

1. When Controller or Processor, based inside of the EU/EEA transfers personal data to a Controller or Processor based in a country outside of the EU/EEA that is not subject to an adequacy decision of the EU commission, both Parties will comply with EU SCC's. In scenarios, where the receiving Party processes personal data on behalf of the other Party, the Parties will comply with the Processor to Controller and Controller to Processor Clauses in Schedule 4. Any Processing of Personal Data. Quasr uses content delivery networks that
2. In such scenario, the provisions of Schedule 4 shall take precedence over the provisions of this DPA.

11. DURATION

This DPA enters into force the date Personal Data is first processed by Processor. This DPA ends automatically on the date of termination or expiry of the Quasr Subscription Agreement, unless the DPA is terminated earlier. The frequency of the processing is continual and ongoing during the term of the Quasr Subscription Agreement.

12. LIABILITY

1. If it can be proven that Quasr has failed to comply with its obligations under this DPA or under the GDPR, Quasr shall be liable for proven direct damage suffered by the Customer. Quasr shall not be liable for indirect, immaterial and/or consequential damages, including loss of profit, loss of opportunity, loss of and/or damage to data, loss of reputation, sanctions and/or fines, and unforeseeable damage. Quasr's liability to the Customer shall in any case be limited to the total amount paid by the Customer to Quasr under the Agreement during the last twelve (12) months.
2. Each Party shall be liable for administrative fines imposed by a supervisory authority in respect of its own Processing.
3. No provision of this DPA shall limit or exclude any liability or right to which the Data Subject may be entitled under law in case of damage resulting from a breach of the GDPR by Quasr in its capacity as Processor.
4. The provisions of this Article are without prejudice to any other provision on liability contained in the Quasr Subscription Agreement.

13. APPLICABLE LAW AND JURISDICTION

This DPA is subject to and shall be interpreted in accordance with the Belgian Data Protection Laws. Disputes arising from this DPA must be brought before the courts as set forth in the Quasr Subscription Agreement.

15. UPDATES

Processor may modify this DPA as required as a result of (a) changes in Applicable Data Protection Laws; (b) a merger, acquisition, corporate reorganization or other similar occurrence; or (c) the release of new features, functions, products or services or material changes to any of the existing Services. Processor may make such modifications by posting a revised version of this DPA at quasr.io/legal/dpa/

and by notifying Controller. Processor will provide at least seven (7) calendar days' advance notice of any modifications. Subject to the seven (7)-calendar day advance notice requirement, the modified version of the DPA will become effective upon posting. Within this seven (7)-calendar day period, the Controller can object to these modifications and the Parties will come to a mutual agreement. By continuing to use the Quasr Platform after the 7-day period, the Controller agrees to be bound by the modified DPA.

Schedules:

Schedule 1: Details of the Personal Data Processing

Schedule 2: List of Sub-processor

Schedule 3: Technical and organizational measures

Schedule 4: Standard contractual clauses

Schedule 1: Details of the Personal Data Processing

NATURE OF THE PROCESSING	The processing of certain personal data by the Processor on behalf of the Controller in relation to allowing access of the Controller's users to the Quasr Platform for the purposes of reviewing software projects submitted to the Quasr Platform.
PURPOSE OF THE PROCESSING	1. Collection of the specified data so that the Processor may provide the Services to the Controller 2. Messaging regarding the Controller's use of the Processor's products and services
TYPE OF PERSONAL DATA	1. Company Data such as Company Name, address, VAT 2. Contract owner Data such as first name, last name, email address and credit card data (related to Self Service) 3. Administrator Data such as first name, last name and email address The data shall not include any 'special category' data as defined under GDPR.
CATEGORIES OF DATA SUBJECTS	Employees, developers, contractors of the Controller.

Schedule 2: List of Sub-processors

The below table provides important information about the identity, location and role of each Sub-processor the Processor uses.

Name	Purpose	Location	Additional information
Stripe Payments Europe Ltd	Payment Processor / Subscription Management	EU	
Google Ireland, Ltd	Cloud Service Gsuite	Global	EU for Storage
Slack Technologies, Ltd	Communication Platform	US	
Amazon Web Services EMEA sarl	Platform Provider	EU (Germany and France)	CDN is Global but no PII is cached
Postman	API Platform and documentation	US	

Schedule 3: Technical and organizational measures

- Usernames (IDs) which could potentially contain personal data (such as names, email, phone number, etc.) are securely hashed using industry best practices inside the Quasr platform. The database holding these hashes is not externally accessible and is internally only accessible by the platform itself and privileged platform administrators.

- Quasr works only with digitized documents that are kept in a secured environment that is only accessible to authorized employees.

- MFA is mandatory for all Quasr applications, to maximize security according to industry best practices and standards

- Logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions, (e.g. granting access on a need-to-know and least privilege basis, use of unique IDs and passwords for all users, periodic review and revoking/changing access promptly when employment terminates or changes in job functions occur).

- System audit or event logging are available on all Quasr Applications

- Password controls designed to manage and control password strength, and usage including prohibiting users from sharing passwords.

- Personal data is only accessible over secured encrypted communication channels (TLS 1.2 or higher).

- Access to the storage locations is limited by AWS security policy.

- Quasr does not allow personal data to be downloaded onto local/personal machines and should at all times remain inside the tools mentioned above.

- Quasr will only work with GDPR compliant subcontractors

- Quasr incorporates Privacy by Design principles for systems and enhancements at the earliest stage of development and serves as one of its core design principles.

Schedule 4: Standard contractual clauses

SECTION I

Clause 1

Purpose and scope

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

(b) The Parties:

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

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

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

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

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

Clause 2

Effect and invariability of the Clauses

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

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

[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 […].

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 - 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.

MODULE TWO: Transfer controller to processor

8.1 Instructions

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

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

8.2 Purpose limitation

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

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[2] (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

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

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

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

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

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

8.9 Documentation and compliance

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

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

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

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

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

MODULE FOUR: Transfer processor to controller

8.1 Instructions

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

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

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

[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 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.

(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter "personal data breach"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data[3], the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

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

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

8.3 Documentation and compliance

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

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

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least [*Specify time period*] 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.[4] The

[3] This includes whether the transfer and further processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences.

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

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

MODULE TWO: Transfer controller to processor

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

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

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

MODULE FOUR: Transfer processor to controller

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

Clause 11

Redress

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

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body[5] 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.]

[5] 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.

MODULE TWO: Transfer controller to processor

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

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

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

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

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

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

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

Clause 12

Liability

MODULE FOUR: Transfer processor to controller

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

MODULE TWO: Transfer controller to processor

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

MODULE TWO: Transfer controller to processor

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE TWO: Transfer controller to processor

(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[6];

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

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

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

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

---

[6] 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.

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three: , if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

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

MODULE TWO: Transfer controller to processor

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

15.1 Notification

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

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

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

[For Module Three: The data exporter shall forward the notification to the controller.]

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

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

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

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

15.2 Review of legality and data minimisation

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

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

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

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

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

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

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

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

(d) [For Modules One, Two and Three: Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.] [For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] The data importer shall certify the deletion of the data to the data exporter. Until the data is

deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

MODULE TWO: Transfer controller to processor

[OPTION 2 (for Modules Two and Three): 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 Belgium.]

MODULE FOUR: Transfer processor to controller

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

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

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

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

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

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

MODULE FOUR: Transfer processor to controller

Any dispute arising from these Clauses shall be resolved by the courts of Antwerp (Belgium).

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

MODULE FOUR: Transfer processor to controller

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

1. Name: …

Address: …

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

Activities relevant to the data transferred under these Clauses: …

Signature and date: …

Role (controller/processor): …

2. …

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

1. Name: …

Address: …

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

Activities relevant to the data transferred under these Clauses: …

Signature and date: …

Role (controller/processor): …

2. …

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

MODULE FOUR: Transfer processor to controller

Categories of data subjects whose personal data is transferred

……..

Categories of personal data transferred

……..

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

……..

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

……

Nature of the processing

……

Purpose(s) of the data transfer and further processing

……..

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

……..

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

……..

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

Identify the competent supervisory authority/ies in accordance with Clause 13

……..

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE TWO: Transfer controller to processor

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

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.

[Examples of possible measures:

Measures of pseudonymisation and encryption of personal data

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

Measures for user identification and authorisation

Measures for the protection of data during transmission

Measures for the protection of data during storage

Measures for ensuring physical security of locations at which personal data are processed

Measures for ensuring events logging

Measures for ensuring system configuration, including default configuration

Measures for internal IT and IT security governance and management

Measures for certification/assurance of processes and products

Measures for ensuring data minimisation

Measures for ensuring data quality

Measures for ensuring limited data retention

Measures for ensuring accountability

Measures for allowing data portability and ensuring erasure]

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

ANNEX III – LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

EXPLANATORY NOTE:

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

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

1. Name: …

Address: …

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

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): …

2. …