EVS BROADCAST EQUIPMENT SA, Rue du Bois Saint-Jean 13, 4102 Seraing, BELGIUM (Register of Legal Entities of Liège 0452.080.178)
EVS BROADCAST EQUIPMENT INC, 3rd Floor, 700 Route 46 East, Fairfield, NJ 07004, USA
EVS BROADCAST EQUIPMENT LTD, Room A 35/F Lee & Man Commercial Center, 169 Electric Road North Point HONG KONG
AXON DIGITAL DESIGN BV, Hercules 28, 5126 RK Gilze, THE NETHERLANDS
AXON DIGITAL DESIGN LTD, C/O Tmf Group 8th Floor, 20 Farringdon Street, London, EC4A 4A, UNITED KINGDOM

DATA PROCESSING ADDENDUM

1. Scope

1.1. This Data Processing Addendum shall apply with the framework the provision of support, trade-in and video production management services (the "services") to be provided by EVS Broadcast Equipment SA or any of its affiliates ("EVS") to you ("Customer") based on existing contractual provisions (the "Principal Agreement") in accordance with the Regulation (EU) 2016/679 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, and repealing Directive 95/46/EC (General Data Protection Regulation – hereinafter the "GDPR"). This Data Processing Addendum supersedes any other terms and conditions of Customer relating to a similar subject matter, even if these have not been specifically rejected by EVS. The provisions of the Principal Agreement that are not expressly modified by this Addendum shall remain unchanged and in force for the duration of the Principal Agreement.

2. Definitions

2.1. Except when expressly specified otherwise in this Addendum, the capitalized terms shall have the meaning set forth in the Principal Agreement.

3. Modifications of the Principal Agreement

It is hereby agreed to add the following provisions to the Principal Agreement in a new Clause related to data protection and privacy:

*" **Data Protection and Privacy***

*1 **Definitions***

For the purposes of this Clause 1, the following capitalized terms shall have the meaning specified below:

*(a) "**Data Protection Law**" shall mean (i) any and all applicable laws implementing the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (as may be modified or replaced), including but not limited to the Belgian law of 8 December 1992 on the protection of individuals regarding the processing of personal data as amended, any directly applicable EU regulations (including but not limited to Regulation (EU) 2016/679 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, and repealing Directive 95/46/EC (General Data Protection Regulation – "**GDPR**") which is applicable as from 25 May 2018) as well as any delegated act in relation to the GDPR, Belgian laws and decrees executing the GDPR and (ii) any similar applicable legislations from countries outside of the European Union.*

*(b) "**Instructions**" means the documented instructions from the Customer to EVS as attached to this Addendum in Annex 1;*

*(c) "**Purposes**" shall mean the limited, specific and legitimate purposes of the Processing, namely the performance of the services;*

*(d) "**Subprocessor**" shall mean any person (excluding an employee of EVS) appointed by or on behalf of EVS to process Personal Data on behalf of Customer in connection with the Principal Agreement;*

(e) The terms, "Controller", "Data Subject", "Personal Data", "Personal Data Breach", "Processing", "Processor" and "Supervisory Authority" shall have the same meaning as in the GDPR.

*2 **Qualification***

For the avoidance of doubt, the Parties acknowledge that where Data Protection Law applies, Customer acts as the Controller and EVS as the Processor of Personal Data to be processed. Accordingly, Customer remains solely responsible for determining the means and the purposes of the EVS' Processing of Personal Data under this Addendum.

*3 **Processing of Personal Data***

Any Processing of Personal Data by EVS in respect of which EVS acts as processor on behalf of Customer shall be carried out in accordance with the Data Protection Law and the provisions of this Clause 3.

Customer agrees to comply with the requirements of the Data Protection Law with respect to the Processing of Personal Data.

Customer warrants that it owns or has obtained all necessary rights and/or consents and provided all necessary notices to Data Subjects as required by applicable Data Protection Law, with respect to any Personal Data and to the extent necessary for the Parties to Process such Personal Data, and that EVS' use of any EVS Personal Data in accordance with the Principal Agreement will not violate any applicable law, rule or regulation. Furthermore, Customer warrants that: (i) EVS' Processing of any Personal Data in accordance with any Customer instruction shall be in compliance with applicable Data Protection Law; and (ii) prior to transmitting Personal Data to EVS, Customer shall inform EVS of any applicable requirements pertaining to the transmitted Personal Data. Customer shall be responsible for all liability and shall indemnify and hold EVS harmless from and against all claims and damages, due to a breach of the foregoing warranties.

Without prejudice to the independence of the Parties, the Personal Data shall only be processed in accordance with the instructions of Customer and solely for the Purposes, to the exclusion of any other purposes. Customer hereby generally instructs EVS to process Personal Data for the Purposes and to the extent necessary to provide the Services in compliance with EVS' obligations under this Addendum.

Without prejudice to the independence of the Parties, EVS represents and warrants that EVS and any person acting under the authority of or on behalf of EVS and having access to the Personal Data shall only process the Personal Data in accordance with the instructions of Customer, except in case of a legal obligation, and in accordance with the Data Protection Law. To this end, EVS shall inform all persons acting under its authority and having access to the Personal Data about the provisions of Data Protection Law.

If the Data Protection Laws apply to the Processing of Personal Data, and Customer is itself a processor, Customer warrants to EVS that Customer's instructions with respect to Personal Data have been authorized by the applicable controller, including the appointment of EVS as another processor or Subprocessor.

*4 **Subprocessing – Onward transfer of Personal Data***

Customer agrees that EVS may use Subprocessors to fulfill its contractual obligations under this DPA or to provide certain services on its behalf, such as providing storage services. Annex 2 lists Subprocessors that are currently engaged by EVS to carry out processing activities on Personal Data on behalf of Customer. Where EVS engages a Subprocessor for carrying out specific processing activities on behalf of Customer, similar protection obligations as contained herein shall be imposed on that Subprocessor by way of a written agreement, in particular providing sufficient guarantees to implement appropriate technical and organisational measures.

With respect to each Subprocessor, EVS shall:

(i) carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level of protection for Personal Data required by this Addendum;

*(ii) ensure that the EU Standard Contractual Clauses regarding the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection (hereinafter the "**EU Standard Contractual Clauses**" - the current template of EU Standard Contractual Clauses is attached to this Addendum as **Annex 3**) are at all relevant times signed between Customer and the Subprocessor, as an attachment to the agreement between EVS and the Subprocessor, if the engagement of such Subprocessor involves a transfer to a country located outside of the European Economic Area which does not ensure an adequate level of data protection and where no appropriate safeguard exists (hereinafter the "**Restricted Transfer**").*

If the Customer reasonably objects to the Processing of Personal Data by one or more Subprocessors, then the Customer shall notify EVS in writing (including e-mail) within 90 (ninety) calendar days after the publication of the use of such Subprocessor on EVS website.

In the event Customer objects to a Subprocessor, EVS will use reasonable efforts to change the affected services or to recommend another commercially reasonable change to the Customer's use of the affected services to avoid the Processing of Personal Data by the Subprocessor concerned. If EVS is unable to make available or propose such change within (60) calendar days, the Customer may terminate the relevant part of the Principal Agreement regarding those services which cannot be provided by EVS without the use of the Subprocessor concerned. To that end, the Customer shall provide written notice of termination taking into account a notice period of 6 months and providing a reasonable motivation for non-approval.

EVS shall not communicate, disclose or transfer, either free of charge or in return for payment, the Personal Data to any other legal person or individual, except where such communication, disclosure or transfer: (i) is necessary to perform the Services or for the Purposes, subject to the limitations set forth in the present Addendum; or (ii) is required by any applicable law, regulation, or governmental authority in which case EVS will, wherever possible, notify Customer promptly in writing prior to complying with any such request for communication, disclosure or transfer and shall comply with all reasonable directions of Customer with respect to such communication, disclosure or transfer.

*5 **Security***

EVS shall ensure – having regard to the state of technological development and the cost of implementing any such measures as well as the sensitive nature of the Personal Data to be processed – that appropriate technical and organizational measures are taken against accidental or unauthorized destruction, accidental loss, as well as against alteration of, access to and

DATA PROCESSING ADDENDUM

any other unauthorized processing of the Personal Data. Without limitation to the foregoing and without prejudice to those obligations contained in the applicable policies (if any) which may be communicated from time to time to EVS, EVS shall, in particular, take adequate technical and organizational measures to:

- *i. ensure that access to the Personal Data is only granted to persons acting under its authority and strictly on a need-to-know basis;*
- *ii. prevent the use of data processing systems by unauthorized persons ;*
- *iii. ensure that the Personal Data cannot be read, copied, modified or removed without authorization EVS during electronic transfer or during transport or storage on data media and that it is possible to check and determine to whom communication of the Personal Data is made through data transfer facilities;*
- *iv. ensure that the Personal Data is only processed in accordance with Customer's instructions;*
- *v. ensure the reliability of any employee, agent or contractor of Customer or any Subprocessor and that they are subject to confidentiality obligations;*
- *vi. ensure that the Personal Data is protected against accidental destruction or loss.*

EVS shall adapt such measures systematically to the development of regulations, technology and other aspects and supplemented with the applicable technical and organizational measures of Subprocessors, as the case may be.

6 ***Cooperation***

EVS shall provide in a prompt manner such co-operation as is reasonably necessary to enable Customer to ensure compliance with the Data Protection Law and to the extent the necessary information is solely in the possession of EVS or its Subprocessors, including but not limited to providing co-operation where Customer must respond to requests for exercising the Data Subject's rights granted by Data Protection Law. In particular, EVS shall:

- *i. without undue delay notify Customer if EVS or any Subprocessor receives a request from a Data Subject under any Data Protection Law in respect of Personal Data; and*
- *ii. ensure that EVS and/or any Subprocessor only responds to such request upon express written instructions of Customer or as required by applicable laws to which EVS and/or the Subprocessor is subject.*

EVS shall conform to any time-scales set out in the Data Protection Law for Data Processor and, if applicable, correct or delete any inaccuracies in Personal Data, as directed by Customer

7 ***Personal Data Breach***

In case of any Personal Data Breach, EVS shall promptly notify Customer of such breach. The notification must, at least, describe the nature of the Personal Data Breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned, describe the likely consequences of the Personal Data Breach, describe the measures taken or proposed to be taken to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

EVS shall co-operate with Customer and take such steps as are directed by Customer to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8 ***Audit and inspection***

EVS shall, at the request of Customer, no more frequently than once annually, make available to Customer information reasonably requested by Customer to demonstrate EVS' compliance with its obligations relating to the Processing of Customer's Personal Data. Such audit shall be performed by Customer or a third party (selected by Customer and reasonably acceptable to EVS) to act on its behalf, at Customer's expense, at EVS' offices or at another mutually agreed location during normal business hours upon thirty (30) days prior written notice and shall make reasonable endeavors to avoid causing any damage, injury, or disruption in EVS' premises, equipment, personnel and business while its personal are on those premises in the course of such an audit or inspection. Audit reports shall only include detail sufficient to verify EVS' compliance with its obligations under this Clause 8.

*For the performance of the audit or inspection, Customer will give a list of authorized person(s) ("**Authorized Person**"). EVS undertakes to give access to its premises to the Authorized Person provided that such Authorized Person:*

- *(i) produces reasonable evidence of identity;*
- *(ii) works during normal business hours of EVS unless the audit needs to be conducted on an emergency basis.*

9 ***Data Protection Impact Assessment***

EVS shall reasonably assist Customer with any relevant data protection impact assessment and prior consultations with Supervisory Authorities or other competent data privacy authorities that would be required under Articles 35 or 36 of the GDPR, subject to terms and conditions and fees to be agreed upon on a case-by-case basis.

10 ***Deletion or return of Personal Data***

EVS shall ensure that any copies of Personal Data in the possession of EVS are promptly, and in any event within one month of the date of potential cessation of any services, returned to Customer or destroyed (at EVS' option) upon Customer's request and/or when they are no longer required for the performance of EVS' obligations under the Principal Agreement, whichever occurs first, and EVS shall delete existing copies unless Data Protection Law requires storage of the Personal Data.

11 ***Liability***

EVS shall be liable for the Processing of the Personal Data which is consigned to it by Customer. EVS undertakes to indemnify and hold harmless Customer, its directors and employees against any and all costs, charges, damages, expenses and losses (including costs incurred in recovering same), that are incurred by Customer as a result of any breach by EVS of any representation or warranty as contained herein or the failure to comply with any of its obligations as contained herein. EVS shall remain in any event fully liable to Customer for the performance of such Subprocessor's obligations. In any event, the aggregate maximum liability of EVS as Processor of Personal Data under the present Addendum shall be limited to the lower of (i) the price paid by the Customer to EVS under the Principal Agreement in the 12-month period immediately preceding the earliest event giving rise to the liability, or (ii) EUR 10,000.

12 ***Modifications of the applicable Data Protection Law***

EVS may, by providing at least thirty (30) calendar days' written notice to the Customer, make variations to or replace the template EU Standard Contractual Clauses included in ***Annex 3*** *and enter into amended or new EU Standard Contractual Clauses as per Clause 4, subsection (ii), where such variations or replacements are required as a result of any change in, or decision of a competent authority under, the Data Protection Law, to allow the Restricted Transfers referred to in Clause 4, subsection (ii), to be made (or continue to be made) in compliance with the Data Protection Law. Each Party may propose any variations to this Addendum where such Party reasonably considers to be necessary to address the requirements of any Data Protection Law.*

4. **Entry into force**

This Addendum enters into force at the date EVS starts providing the Services to Customer and remains into force for the entire duration of the Principal Agreement.

ANNEX 1: Instructions

1. *Nature and purpose of the Processing: Personal Data will be Processed for the purposes of the performance of the services under the Principal Agreement including the following purposes:*
   - *a) Provision of appropriate support services depending on the issue at stake*
   - *b) Provision of video production management services*
   - *c) Provision of appropriate trade-in services*
   - *d) Management and follow-up of Customer's requests, history and equipment in this respect*
   - *e) Provision of Software as a Service*
   - *f) Continuous improvement of the services*
   - *g) Compliance with Data Protection Law, information security requirements and service level agreements*
   - *h) Claims management with and between the Customer, EVS, the Data Subject(s) and/or third parties, including beyond termination of the Agreement for any reason whatsoever*
   - *i) Any other purpose of Processing of Personal Data agreed upon between Parties in the relevant statement of work or any other document of the Principal Agreement.*
2. *Type of Personal Data: The Personal Data transferred concerns all relevant information that is required to deliver the requested services, which may include (a subset of) the following categories of data:*
   - *a) Personal details such as name, birth date, etc.*
   - *b) Contact details such as address, e-mail address, telephone number, etc.*
   - *c) Authentication Credentials to use the Services, such as username, IP address, PC Name, etc.*

DATA PROCESSING ADDENDUM

d) Activities performed by Customer users in their use of the Services and/or SaaS.
e) Video content and images, and data related to it (thubnails, metadata, etc.).
f) Any other category of Personal Data agreed upon between Parties in the relevant statement of work or any other document of the Principal Agreement.

3. *Categories of Data Subject: employees and consultant of the Customer and if applicable, persons identified or identifiable through Customer's video content and images.*
4. *Duration of the Processing: The duration during which the Processing of Personal Data by EVS is allowed corresponds the duration of the Principal Agreement.*
5. *Permitted purposes: All the Processing strictly necessary with regard to the nature and purpose of the Processing, as set forth in section 1 of the present Annex 1 including: data consultation, storage, etc.*

ANNEX 2: EVS SUBPROCESSORS

Support, rental: No subprocessor

C-Cast: AWS Cloud

MediaHub:
AWS Cloud
Alibaba
GTT (Interroute)
Wasabi
Google analytics
Aspera
NSI Software Services
Approach
Blackbird

ANNEX 2: EU STANDARD CONTRACTUAL CLAUSES

Based on the Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council
Based on the Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council
MODULE THREE: Transfer processor to processor

SECTION I

Clause 1 Purpose and scope

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

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 –: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);
(iii) Clause 9 –Module Three: Clause 9(a), (c), (d) and (e);
(iv) Clause 12 –: Clause 12(a), (d) and (f);
(v) Clause 13;
(vi) Clause 15.1(c), (d) and (e);
(vii) Clause 16(e);
(viii) Clause 18 –: Clause 18(a) and (b).
(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4 Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5 Hierarchy

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

Clause 6 Description of the transfer(s)

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

Clause 7 – Optional Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8 Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.
8.1 Instructions
(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.
(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.
(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.
(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter (5).
8.2 Purpose limitation
The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.
8.3 Transparency

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

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

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

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

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

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

8.7 Sensitive data

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

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (6) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

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

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

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

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

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

8.9 Documentation and compliance

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

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

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

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

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

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

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

Clause 9 Use of sub-processors

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

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. (9) 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.

DATA PROCESSING ADDENDUM

(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10 Data subject rights

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.
(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

Clause 11 Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
(ii) refer the dispute to the competent courts within the meaning of Clause 18.
(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12 Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.
(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13 Supervision

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.
[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.
[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.
(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

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

Clause 14 Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards (12);
(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

DATA PROCESSING ADDENDUM

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.]
(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.
[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

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Belgium (specify Member State).

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 Liège, Belgium (specify Member State).
(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
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]
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): …

DATA PROCESSING ADDENDUM

Data importer(s): [Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]
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): …
B. DESCRIPTION OF TRANSFER
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
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
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.